



A MITEL
PRODUCT
GUIDE

MiVoice Business

EX Controller Installation and Administration Guide

Release 10.5

Document Version 1.0

October 2025

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks Corporation (MITEL[®])**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC), its affiliates, parents, or subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: <http://www.mitel.com/trademarks>.

[®], [™] Trademark of Mitel Networks Corporation

© Copyright 2025, Mitel Networks Corporation

All rights reserved

Contents

1 About this Guide.....	1
2 About EX Controller.....	4
2.1 Overview.....	4
2.2 EX Controller Architecture.....	5
2.3 User Interfaces.....	6
2.4 Supported Hardware Configuration.....	11
2.4.1 Sample Configuration.....	11
2.4.2 Optional Accessory.....	11
2.5 Models and Part Numbers.....	12
2.6 Specifications.....	13
2.6.1 Operating Environment.....	13
2.6.2 Storage Temperature.....	13
2.6.3 Dimensions and Weight.....	13
2.6.4 Connection Interfaces and LEDs.....	14
3 Hardware Installation.....	19
3.1 Overview.....	19
3.2 Package Checklist.....	19
3.3 Requirements.....	20
3.3.1 Location.....	20
3.3.2 Wiring.....	20
3.3.3 Tools and Equipment.....	21
3.4 Installation Checklist.....	21
3.5 Cleaning Instructions.....	22
3.6 Installing the EX Controller.....	22
3.6.1 EX Controller 16/120G Dual PS.....	23
3.7 Installing Telephony Cards.....	26
3.8 Cabling.....	28
4 Software Installation.....	29
4.1 Overview.....	29
4.1.1 PC Requirements.....	29
4.2 Prerequisites.....	30
4.3 Accessing the EX Controller Deployment Tool.....	31
4.4 Updating the EX Controller Deployment Tool.....	32
4.5 Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine.....	34
4.6 Post-Installation Tasks.....	42
4.6.1 Default Passwords.....	42
4.6.2 Log into Server Manager.....	43

4.6.3 Licensing the MiVoice Business system.....	44
4.6.4 Log into the MiVoice Business System Administration Tool.....	44
4.6.5 Log in to the EX Controller Web GUI.....	47
4.6.6 Program the MiVoice Business System.....	48
4.6.7 Trunk Configuration.....	49
4.7 Enabling the VNC Capability.....	50

5 Maintenance.....52

5.1 Software Upgrade.....	52
5.1.1 Prerequisite.....	52
5.1.2 Procedure.....	53
5.1.3 Upgrade with Remote Fresh Install Blade.....	53
5.1.4 Restoring an EX from a Server Manager Backup.....	56
5.1.5 Mount Software Blade on Server Manager Manually.....	57
5.2 Backup and Restore.....	58
5.2.1 Backup and Restore Using Server Manager.....	58
5.2.2 Backup and Restore Using MiVoice Business System Administration Tool.....	58
5.3 Field Replaceable Units.....	59
5.3.1 Cooling Fan/Power Supply/Solid State Drive.....	59
5.3.2 Telephony Cards.....	59
5.4 Change IP Address of the EX Controller Web GUI.....	61
5.5 Configure the Server Using Server Console.....	63
5.5.1 Accessing Server Console.....	63
5.5.2 Configure this Server.....	65
5.5.3 Manage trusted networks.....	68
5.5.4 Perform backup.....	69
5.5.5 Verifying a Backup File.....	70

6 Troubleshooting..... 72

6.1 System Software.....	72
6.2 Reset/Default Button.....	78
6.2.1 Partial Reset.....	78
6.2.2 Factory Reset.....	81
6.3 Reset the System Administration Tool Password.....	85

7 Appendix A: Assigning a Static IP Address to the EX Controller Deployment Tool.....87

7.1 Assigning a static IP address manually.....	87
7.2 Assigning a static IP address by using a USB flash drive.....	95

8 Appendix B: Programming R2 Trunks.....98

9 Appendix C: Enabling USB Ports for the Deployment Tool..... 105

10 Appendix D: Increasing the RAM size for MiVoice Business Virtual Machine..... 109

11 Appendix E- Programming Enterprise Gateway Trunks and Analogue FXS Ports.....	112
12 Appendix F - Enabling/Disabling VNC Capability and Resetting the MSL Password.....	116
12.1 Enabling the VNC Capability.....	116
12.2 Disabling the VNC Capability.....	116
12.3 Resetting the MSL password.....	117
13 Appendix G - EX-Controller Link Redundancy support.....	119

About this Guide

1

The EX Controller Installation and Administration Guide is intended for certified MiVoice Business technicians who are installing, upgrading, maintaining, and troubleshooting the Mitel® MiVoice Business software deployed on an EX Controller.

What's New in This Document

This section describes changes in this document due to new and changed functionality in EX Controller Release 10.5. The changes are summarized in the following table.

Table 1: Document Version 1.0

Feature/ Enhancement	Document Updates	Location	Publishing Date
The user should not reboot the EX controller while deploying MiVoice Business deployment.	Added a Note to notify the user.	Section 4.5 Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine	October 2025

Related Documents

Document Title	Description	Location
General Information Guide	Provides an overview of the MiVoice Business system.	Document Center
Troubleshooting Guide	Provides troubleshooting instructions related to MiVoice Business.	Document Center
MiVoice Business Migration Guidelines	Provides guidelines for preparing and migrating your MiVoice Business system to MiVoice Business Release 9.0 or later, or to another platform.	Document Center

Document Title	Description	Location
EX Controller and GX Gateway Safety Instructions	Provides basic installation information, necessary for the proper and safe functioning of this equipment.	Document Center
MiVoice Business Engineering Guidelines	Provides guidelines for planning an installation of a MiVoice Business Communications Platform.	Document Center
MiVoice Business Security Guidelines	Provides guidelines for secure deployment and secure operation of the MiVoice Business (MiVoice Business) system.	Document Center
Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines	Provides information about network cabling and guidelines for twisted pair cabling installation.	Document Center
Mitel IP Sets Engineering Guidelines	Provides guidelines for individuals who are planning for the installation of Mitel IP phones.	Document Center
Network Engineering for IP Telephony	Provides guidelines that should be considered prior to deploying IP phones, such as network design, QoS mechanisms and related protocols.	Document Center
AG4124 Analog Gateway Administration Guide	Provides information about the AG4124 Analog Gateway, including instructions on how to install, configure, and use the Analog Gateway.	Document Center

Contacting Mitel Technical Support

Keep the following information handy when you contact the Mitel Technical Support:

- MiVoice Business software version installed or trying to install
- DGW firmware version
- EX Controller Deployment Tool version number or the exdeploy zip file (exdeploy-x.x.x.x.zip) version number

- Product serial number
- Nature of the problem
- What you were doing with the application when the problem occurred
- Troubleshooting results

For information about contacting Mitel Technical Support:

1. Go to [Mitel MiAccess](#), and in the left navigation pane, click **InfoChannel**.
2. In the **Select Infochannel** drop-down, click **Mitel - Worldwide**.
3. In the left navigation pane, click **Services and Support > Support Services**.
4. Under **Support Services**, click **Technical Support**.
5. Under **Technical Support**, click **Contacting Mitel Technical Support**.

The Contacting Mitel Technical Support page is displayed that describes various ways to contact Mitel Technical Support.

About EX Controller

2

This chapter contains the following sections:

- [Overview](#)
- [EX Controller Architecture](#)
- [User Interfaces](#)
- [Supported Hardware Configuration](#)
- [Models and Part Numbers](#)
- [Specifications](#)

2.1 Overview

The EX Controller is a hardware platform that supports the MiVoice Business call processing software. The EX Controller supports up to 1400 IP users and provides analog capabilities of up to 28 Foreign Exchange Subscriber (FXS) or Foreign Exchange office (FXO) ports or 8 T1/E1 ports.

Important:

The architecture and deployment of the EX Controller is different from MiVoice Business 3300 Integrated Communication Platform (ICP) controllers. Strictly follow the deployment procedures provided in this document to avoid issues with deployment.

The following table lists the difference between the EX Controller 8/120G Dual PS and the EX Controller 16/120G Dual PS:

Specifications	EX Controller 4/60G	EX Controller 8/120G Dual PS	EX Controller 16/120G Dual PS
CPU	Intel Celeron N2930	Intel Celeron N2930	AMD Ryzen V1605B
Storage (SSD)	60 GB	120 GB	120 GB
RAM	4 GB	8 GB	16 GB
CPU Cores/Threads/ Threads Available for Mitel VM Usage		4/4/3	4/8/7

EX-solution have two different platforms:

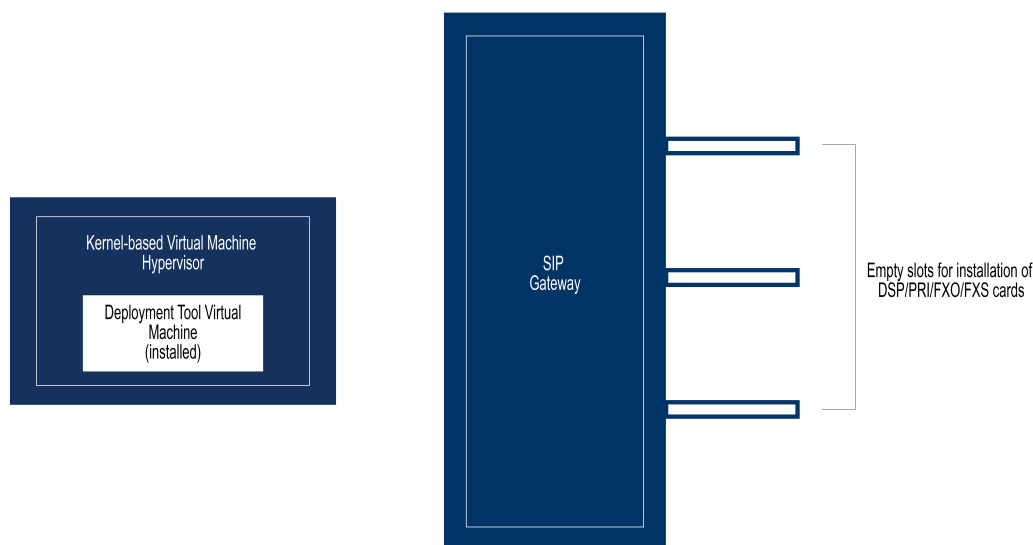
1. The EX host hardware
2. The MiVB Virtual Machine

2.2 EX Controller Architecture

The EX Controller is shipped from the factory with the Deployment Tool installed as a virtual machine on a Kernel-based Virtual Machine (KVM) hypervisor.

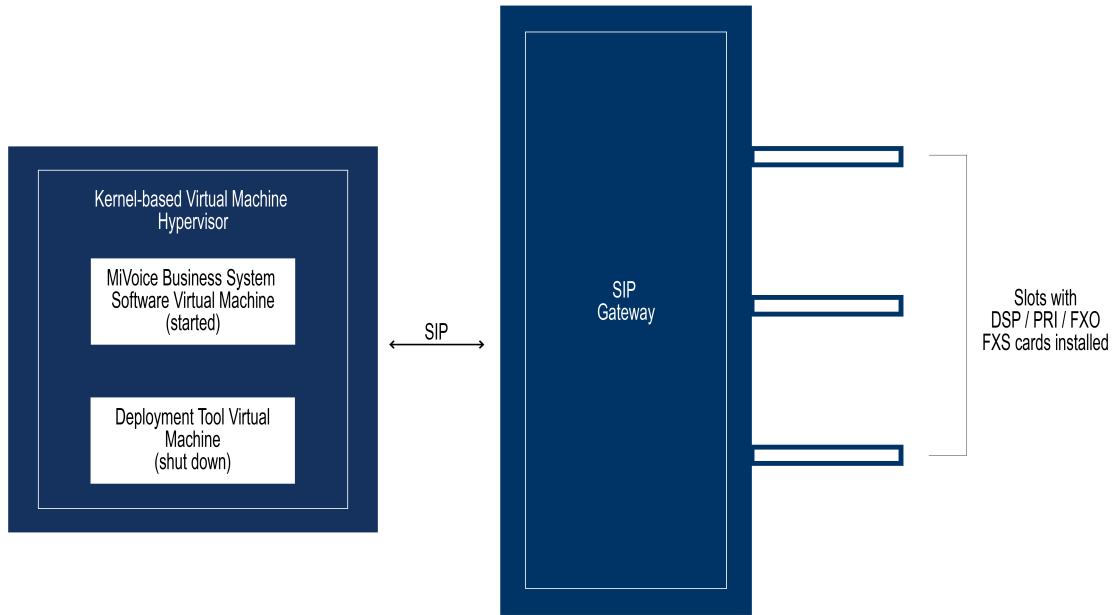
Note: As the EX controller does not support 802.1Q VLAN Trunks, the EX controller does not set an 802.1p Ethernet priority. The EX controller will use DSCP information to provide priority information in packets sent at layer 3. However, Ethernet Priority information and VLAN assignment must be configured at the first access port of the Ethernet switch because data will be assigned to an untagged VLAN, which is usually VLAN 1. Voice can be prioritized using the DSCP value, which can also be used to identify the Ethernet priority value set in the DSCP to Priority map in the Ethernet switch. This is also known as QoS to CoS mapping. For more details, contact your LAN switch vendor. For more examples, refer to the [MiVoice Business Engineering Guidelines](#).

The following is a graphical representation of the EX Controller (factory) architecture.



The Deployment Tool is a web-based application that is used for deploying the MiVoice Business virtual machine on the EX Controller.

The following is a graphical representation of the EX Controller architecture after deploying the MiVoice Business system software.



After the deployment, the controller shuts down the Deployment Tool virtual machine and starts the MiVoice Business virtual machine. The MiVoice Business virtual machine provides access to the MiVoice Business system software through a browser-based interface called the MiVoice Business System Administration Tool. The System Administration Tool is used for programming the MiVoice Business system. The SIP Gateway facilitates the communication between PRI/FXO/FXS cards and the MiVoice Business system (call server). For more information about the MiVoice Business system, see the *General Information Guide*.

2.3 User Interfaces

The EX Controller has the following user interfaces:

- Deployment Tool
- Server Manager
- MiVoice Business System Administration Tool
- Mitel Configuration Wizard (MiCW)
- EX Controller Web GUI

Deployment Tool

The Deployment Tool is a web-based application that is used for deploying the MiVoice Business system software on the EX Controller. The Deployment Tool is available during the deployment.

Mitel EX Controller Deployment - Fully deployed

Help | Update | Reboot v1.1.27-0

Idle - No existing deployment session

Recall Progress

Platform variant

Call Manager type: MIVB

Call Manager image: Browse... No file selected.

General Settings

ARID: Enter the ARID

Call Manager FQDN: coyotr.acme.com

Distinguished name: cn=coyote, ou=Finance, o=ACME, l=Bangor, st=Maine, c=US

IPv4 DNS servers: 192.168.3.1

IPv4 trusted network address: 192.168.3.0/24

Restore via console: ☐

Enable secure EX Controller access: ☐

LAN Settings

IPv4 EX Controller LAN address: 192.168.3.55/24

IPv4 Call Manager LAN address: 192.168.3.56

IPv4 default LAN gateway: 192.168.3.1

Full deploy | Partial deploy | Finish deploy

Note:

Systems running on Deployment Tool older than 1.1.13, must upgrade to the version 1.1.13 or higher and [enable the USB ports manually](#).

Server Manager

Server Manager is a web-based application that allows you to perform administrative tasks on the MiVoice Business system. Server Manager is available after the deployment.

Mitel | **MiVoice Business** admin@mn204.mitel.com Status: **Clear**

ServiceLink
 Blades
 Status

Administration
 Web services
 Backup
 Restore
 View log files
 Event viewer
 System information
 System users
 Shutdown or reboot

Security
 Remote access
 Syslog
 Web Server

Configuration
 Networks
 E-mail settings
 Google Apps
 DHCP
 Date and Time
 Hostnames and addresses
 Domains
 IPv6-in-IPv4 Tunnel
 SNMP
 Ethernet Cards
 Review configuration

Miscellaneous
 Support and licensing
 Help

EX Platform
 Reboot

Welcome to the server manager

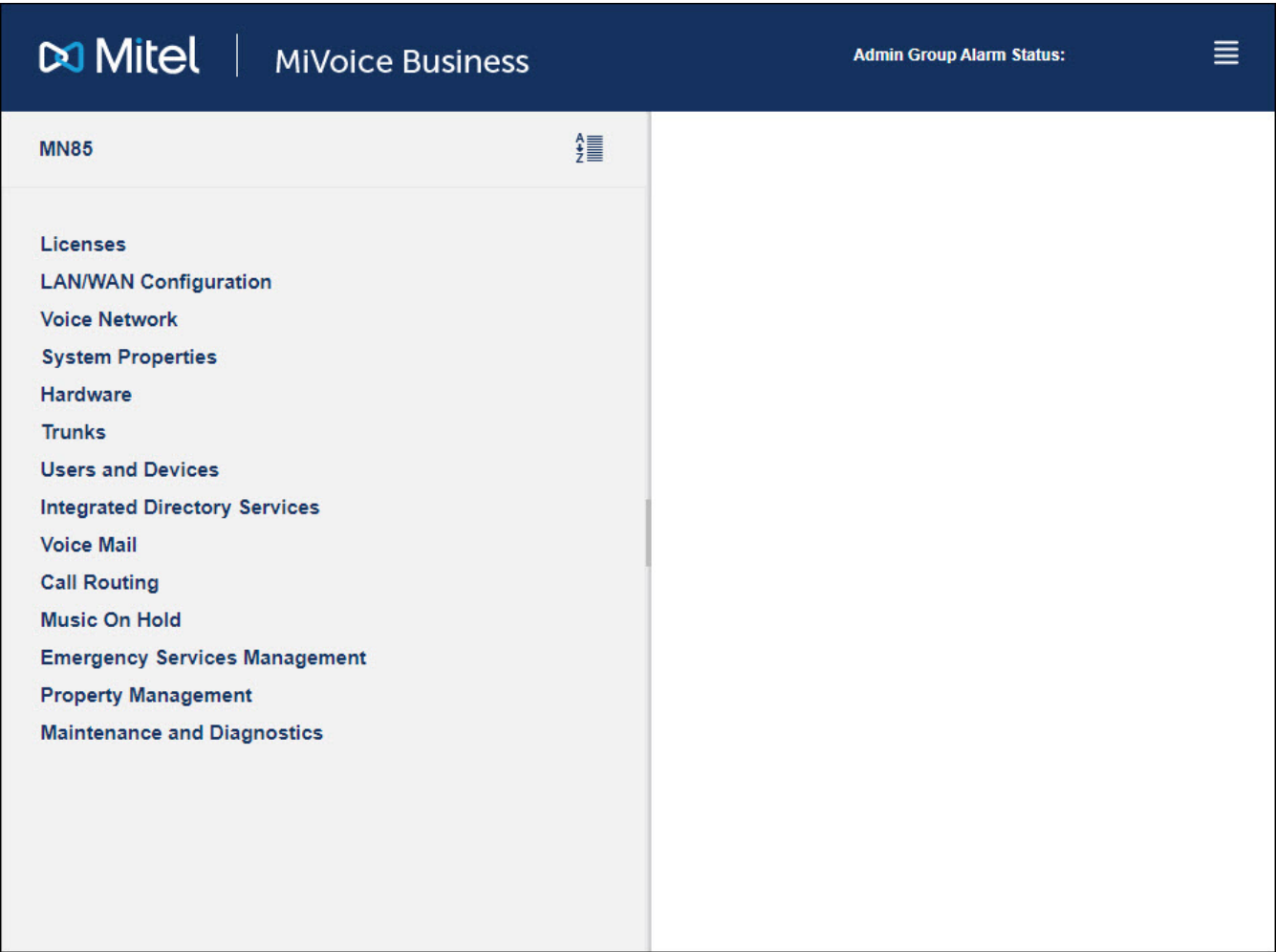
This server is a very secure, reliable and cost-effective platform for an expanding range of business applications and services. For information about the specific applications available for this platform, please contact your authorized reseller.

To perform a system administration function, click one of the links in the menu on the left of your screen.

MiVoice Business 9.1.0.68
 © Mitel Networks Corporation

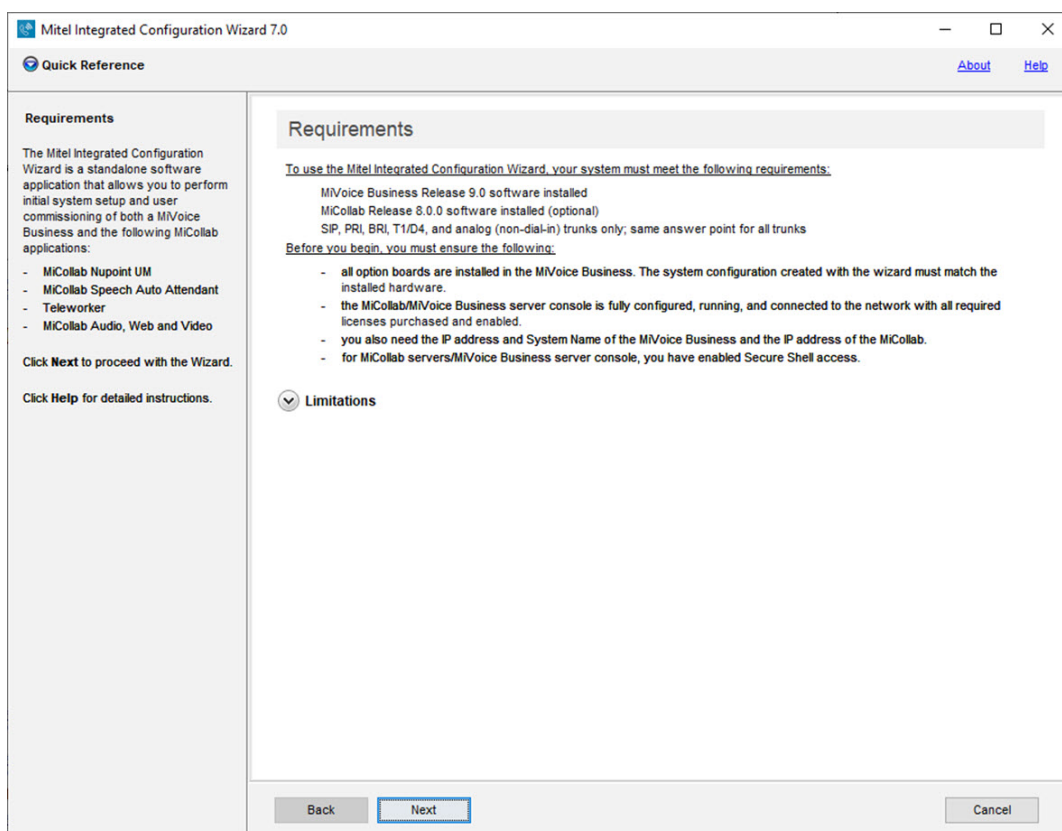
MiVoice Business System Administration Tool

The MiVoice Business System Administration Tool is a web-based application that is used for programming the MiVoice Business system (call programming). The MiVoice Business System Administration Tool is available after the deployment.



Mitel Integrated Configuration Wizard

The Mitel Integrated Configuration Wizard (MiCW) allows you to perform initial system setup and user commissioning of a MiVoice Business platform. The MiCW is available after the deployment.



EX Controller Web GUI

The EX Controller Web GUI is a web-based application that is typically used only for troubleshooting purposes. The EX Controller Web GUI is available after the deployment.

Important:

Do **NOT** use this interface for programming trunks or the MiVoice Business system.

Mitel | EX Controller

System Network SBC Management Reboot

Information Services Hardware Event Log Local Log Packet Capture Diagnostic VM

• Information

Current Status	
Device Identification:	EX Controller
Firmware:	Dgw 44.3.1746
Profile:	STNL-MT-D2000-155
MAC Address:	0090B0bdc8
Serial Number:	000400001M318170017
Number of DSPs:	0
Storage Memory (in use/total):	18.3 GB / 60 GB
Volatile Memory (in use/total):	2.3 GB / 8 GB
System Uptime (D:HH:MM:SS):	12:19:04:19
System Time (DD/MM/YYYY HH:MM:SS):	28/11/2019 02:34:15

Licenses	
CVMP/TR-069	
SBC Licence for 3 concurrent sessions	
Virtual Machine Licence	

Activate Licence	
Licence Key:	

Apply

2.4 Supported Hardware Configuration

The EX Controller has eight slots for accommodating the following cards:

- 1 port PRI (T1/E1) card
- 1 DSP card (required one per chassis when using an FXS or FXO card)
- 4 port FXS card
- 4 port FXO card

2.4.1 Sample Configuration

A sample EX Controller configuration has:

- 2 PRI cards
- 1 DSP card
- 4 FXS cards (providing 16 FXS ports)
- 1 FXO card (providing 4 FXO trunks)

2.4.2 Optional Accessory

A Linux-compatible USB audio is required to support an external Music on Hold source. Mitel recommends using [Pluggable USB Audio Adapter](#). The USB audio can be plugged into, USB1 or USB2 port of the EX Controller.

2.5 Models and Part Numbers

The following table lists the supported EX Controller models and their part numbers.

Part Number	Model
50008375	EX Controller 16/120G Dual PS
50008229	EX Controller with 4 GB RAM and 60 GB storage
50008230	EX Controller with 8 GB RAM, 120 GB storage, and Dual PSU

The following table describes the supported telephony cards for an EX Controller.

Part Number	Telephony Card
50008234	DSP card
50008233	one Port PRI card
50008231	Four Port FXS card, loop limit of 450 m
50008232	Four Port FXO card
51309241	Four Port FXS-LP for EX Controller
50008353	FXO card for Australia

Note:

The following requirements apply only to Australia:

- FXS wiring cannot be bundled with any network cabling. FXS port wiring must be routed in separate cables away from any network cables.
- The FXO interface is voice only, and does not support FAX or modem.
- The FXS and the FXS-LP (available in Q1 2021) interfaces are installed on-premise only.

2.6 Specifications

2.6.1 Operating Environment

- Operating temperature range 0 °C (0 ° F) to +40 °C (104 ° F)
- Humidity maximum 85% and non-condensing

2.6.2 Storage Temperature

-20 °C (-4 °F) to +70 °C (158 °F)

2.6.3 Dimensions and Weight

PARAMETER	DESCRIPTION
Dimensions	Height: 4.4 cm (1.75 in.) Width: 48.3 cm (19 in.) Depth: 36.5 cm (14.4 in.)
Weight	5.4 kg (11.9 lb.) – Single Power Supply 5.85 kg (12.9 lb.) – Dual Power Supply

2.6.4 Connection Interfaces and LEDs



Table 2: LEDs

#	LED	LED State	Description
1	Unit with Power 1 connector only	Green, blinking 1 cycle per second, 50% duty	Unit is being restarted.
		Green, steady on	Unit is restarted.
		off	No current or failing power supply.
1 and 2	Unit with power 1 and power 2 connectors	Green, blinking 1 cycle per second, 50% duty	Unit is being restarted. Unit is restarted.
		Green, steady on	Unit is restarted.
		one LED red, steady on	No current or failing power supply on the power connector.
		Both LEDs off	No current or failing power supply on both power connectors.
3	Ready	Green, steady on	All lines are enabled (operational state).
		Green, steady off	All lines are disabled (operational state).

#	LED	LED State	Description
		Green, blinking 1 cycle per 4 seconds, 75% duty	At least one line is enabled and at least one line is disabled (operational state).
5	In-Use	Off	Lines are idled and unlocked.
		Yellow, steady on	Lines are in use and unlocked.
		Yellow, blinking 1 cycle per second, 50% duty	Locked
10	Link	Green, steady on	Indicates that the PRI port is connected, and the link is up.
		Off	Indicates that the PRI port is not connected, and the link is down.
10	In-Use	Amber, steady on	Indicates that the PRI port is connected.
		Off	Indicates that the PRI port is not connected.
10	Error/Trouble	Red, steady ON	Indicates that the PRI port is not working properly.
		Off	Indicates that the PRI port is working properly.
11	Ready	Amber steady ON	Indicates that the DSP card is ready to send and receive calls.
		Off	Indicates that the DSP card is not connected.

#	LED	LED State	Description
13	ETH1 - Right LED (activity)	Green blinking, variable rate	Connected with active network traffic.
		Green steady on	Connected with no network traffic.
		Off	Not connected
13	ETH1 -Left LED (speed)	Off	10 Mbps
		Green	100 Mbps
		Yellow	1000 Mbps
14	ETH2/3/4/5/ext -Right LED (activity)	Green blinking, variable rate	Connected with active network traffic.
		Green, steady on	Connected with no active network traffic.
		Off	Not connected
14	ETH2/3/4/5/ext -Left LED (speed)	Off	10 Mbps
		Green	100 Mbps
		Yellow	1000 Mbps

Table 3: Switch

#	Switch	Description		
4	Reset/Default	Pressing Duration	Result	LED Pattern

#	Switch	Description		
		2 to 6 seconds	/entry> PoRestarts the EX Controller unit.	

Table 4: Connectors and Cards

#	Connectors/Cards	Description
6	USB1	USB connector
7	USB2	USB connector
8	SYNC IN	8 KHz TDM synchronization pulse input
9	SYNC OUT	8 KHz TDM synchronization pulse output
11	DSP card	No connector available
18	PRI card with PRI port	RJ-48 connector for ISDN-PRI connectivity
12	FXS card with FXS ports	RJ-11 connectors to attach a conventional telephone or G3 fax
13	ETH1	A 10/100/1000 BaseT Ethernet RJ-45 connector for access to a LAN, WAN, or computer. This port is by default used for uplink / WAN connection.
14	ETH2-ETH3-ETH4/EXT-ETH5/EXT	10/100/1000 BaseT Ethernet RJ-45 connector for access to a LAN, WAN or computer. These ports are used by default for LAN connections.

#	Connectors/Cards	Description
16	FXO card with FXO ports	RJ-11 connectors offering analog PSTN access for various VoIP endpoints such as IP phones, FXS devices, softphones and IP-based PBX.

Hardware Installation

3

This chapter contains the following sections:

- [Overview](#)
- [Package Checklist](#)
- [Requirements](#)
- [Installation Checklist](#)
- [Cleaning Instructions](#)
- [Installing the EX Controller](#)
- [Installing Telephony Cards](#)
- [Cabling](#)

3.1 Overview

This chapter describes the following procedures that must be performed sequentially to complete the hardware installation:

1. [Installing the EX Controller](#) on page 22
2. [Installing Telephony Cards](#) on page 26
3. [Cabling](#) on page 28

3.2 Package Checklist

Item	Condition
EX Controller (Qty 1)	
Power cord with the proper model for the country (Qty 1)* *Qty 2 for EX Controller with dual power supply unit.	
Chassis rack mounting bracket (Qty 2)	
Chassis rack mounting bracket screws (Qty 2)	

Item	Condition
Ethernet patch cable, CAT-5E, 7 feet (Qty 1)	
Polyurethane self-adhesive black cylindrical bumper (Qty 1)	
EX Controller and GX Gateway Safety Instructions document (Qty1)	

3.3 Requirements

3.3.1 Location

- Install the controller:
 - In a standard 48.26 cm (19 in.) equipment rack
 - On a flat surface (such as a desk or a table)
- Do not install the controller in a location exposed to direct sunlight or near stoves or radiators. Excessive heat could damage the internal components.
- The controller should be positioned to be accessible for future upgrade, maintenance, and troubleshooting and where cables can be easily connected.
- Maintain a minimum of 25 mm (1 in.) clearance in the front, back, on top, under, and on sides of the controller.
- Keep airflow around and through the vents of the controller clear of any obstruction.

3.3.2 Wiring

These guidelines apply Ethernet cables, supplied or not, used with an EX Controller.

- Category 5 cables can be used for 10/100 Base T-Connections.
- Category 5e or 6 cables are recommended for Gigabyte Ethernet.
- Always use straight-through cables.
- Cables must not pull or create a lateral stress on the connectors; that is, they must be long enough.
- Cables must be installed in such a way the personnel working in the vicinity of the equipment do not trip on them.
- Keep cables away from:
 - Sources of electrical noise such as radios, transmitters, and broadband amplifiers
 - Power lines
 - Fluorescent lighting fixtures
 - Liquids or moisture
 - Heat sources

For more information, see *Ethernet Twisted Pair Cabling Plant, Power and Grounding Guidelines*.

3.3.3 Tools and Equipment

- Screwdriver as required for attaching brackets to rack
- ESD wrist strap
- Earth ground cable

Warning:

The earth ground cable should be the same size (18 AWG minimum) as the earth cable of the provided power cord. Otherwise, make sure the earth ground cable meets the standards and requirements of your local electrical code. The type of the cable is likely to have VW-1 or RT1 markings on the cable.

- RJ45 cables for LAN connections
- RJ48 cables for PRI connections
- RJ11 cables for FXS and FXO connections

3.4 Installation Checklist

Task	Verified by	Date
Network information available and recorded in site log.		
Location requirements verified.		
Site power Voltage		
Installation site pre-power check completed.		
Mounting tools and equipment available.		
Additional equipment available.		
EX Controller received.		
Regulatory compliance and safety information received.		

Task	Verified by	Date
Warranty card received.		
Software version verified (download the latest Deployment Tool)		
Rack, desktop mounting of chassis completed.		
Initial electrical connections established.		
Cable length limits verified.		
Initial configuration performed.		
Initial operation verified.		

3.5 Cleaning Instructions

To clean an EX Controller, wipe with a soft dry cloth.



CAUTION:

Do not use volatile liquids such as benzene or thinner as they can damage the unit's casing.

For resistant markings, wet a cloth with a mild detergent, wring well and then wipe off. Use a dry cloth to dry the surface.

3.6 Installing the EX Controller

Important:

Before installing, ensure that you have read the **EX Controller and GX Gateway Safety Instructions** document supplied with the controller.

To install an EX Controller on a flat surface or in a rack:

1. Make a note or take a picture of your unit's serial number before you begin the installation. The serial number is located underneath the EX Controller casing.
2. Unpack the controller and go through the [Package Checklist](#) on page 19.
3. Apply the polyurethane self-adhesive black cylindrical bumper protective products to the bottom of the controller. This will improve the airflow under the controller.

Note:

Skip this step if you are installing the controller in a rack.

4. Install the controller on a flat surface or in a rack, making sure that the unit is at 20 cm (8 in.) from your monitor, computer casing, or other peripheral, including speakers.

3.6.1 EX Controller 16/120G Dual PS

EX Controller 16/120G Dual PS is available for the Mivoice Business version 9.4 and later.

Prerequisites

- DGW Firmware 48.4 and later versions.
 - DGW Firmware 48.4 and later versions is required to run the **EX Controller 16/120G Dual PS**.

Procedure

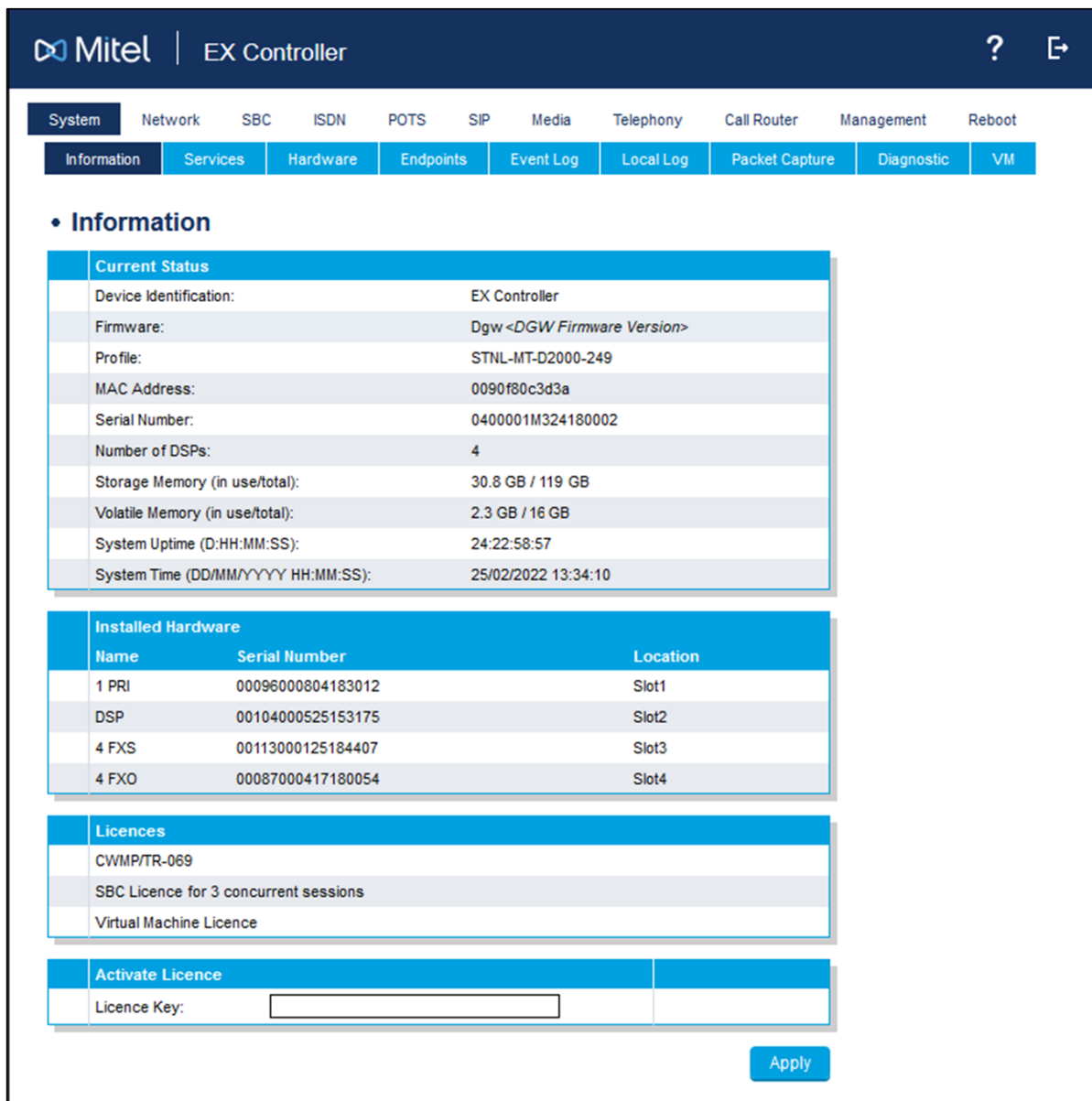
Follow the steps in the section [Procedure](#) to check and enable the USB port for the Deployment Tool.

Note:

The data can be backed up from the existing/older version of MiVB EX to restore on 9.4 with the same set of analog cards.

Identifying the EX Controller 16/120G Dual PC

1. From EX Controller UI navigate to **System > Information**, the field **Volatile Memory (in use/ total)** must display 16GB as the **total**.



The screenshot shows the Mitel EX Controller web interface. The top navigation bar includes tabs for System, Network, SBC, ISDN, POTS, SIP, Media, Telephony, Call Router, Management, and Reboot. The 'System' tab is selected, and the 'Information' sub-tab is active. The main content area is titled '• Information' and contains three sections:

- Current Status**: A table showing system details.

Device Identification:	EX Controller
Firmware:	Dgw <DGW Firmware Version>
Profile:	STNL-MT-D2000-249
MAC Address:	0090f80c3d3a
Serial Number:	0400001M324180002
Number of DSPs:	4
Storage Memory (in use/total):	30.8 GB / 119 GB
Volatile Memory (in use/total):	2.3 GB / 16 GB
System Uptime (D:HH:MM:SS):	24:22:58:57
System Time (DD/MM/YYYY HH:MM:SS):	25/02/2022 13:34:10
- Installed Hardware**: A table listing hardware components.

Name	Serial Number	Location
1 PRI	00096000804183012	Slot1
DSP	00104000525153175	Slot2
4 FXS	00113000125184407	Slot3
4 FXO	00087000417180054	Slot4
- Licences**: A section showing license information.

CWMP/TR-069
SBC Licence for 3 concurrent sessions
Virtual Machine Licence

At the bottom, there is an 'Activate Licence' section with a 'Licence Key:' label and an input field. An 'Apply' button is located at the bottom right of the page.

EX Controller 16/120G Dual PC


EX Controller

System
Network
SBC
ISDN
POTS
SIP
Media
Telephony
Call Router
Management
Reboot

Information
Services
Hardware
Endpoints
Event Log
Local Log
Packet Capture
Diagnostic
VM

• Information

Current Status	
Device Identification:	EX Controller
Firmware:	Dgw 48.4.2631-2-g3e0479843
Profile:	STNL-MT-D2000-294
MAC Address:	0090f80bdc8
Serial Number:	000400001M318170017
Number of DSPs:	4
Storage Memory (in use/total):	20.8 GB / 60 GB
Volatile Memory (in use/total):	3.4 GB / 8 GB
System Uptime (D:HH:MM:SS):	21:23:25:09
System Time (DD/MM/YYYY HH:MM:SS):	19/04/2022 03:16:59

Installed Hardware		
Name	Serial Number	Location
1 PRI	00096000706174223	Slot1
DSP	00104000523154500	Slot2
4 FXS	00085000412161818	Slot3
4 FXO	00087000345140604	Slot4

Licences	
CWMP/TR-069	
SBC Licence for 3 concurrent sessions	
Virtual Machine Licence	

Activate Licence	
Licence Key:	

Apply

EX Controller 8/120G Dual PS

2. On the EX Controller chassis, the label on the front right corner, bearing the Mitel part number is displayed.

Part Number	Model
50008375	EX Controller 16/120G Dual PS



3.7 Installing Telephony Cards

To install telephony cards:

1. Ensure that adequate earth ground connection has been made between the grounding screw on the back of the controller and an appropriate grounding point in your site.

Warning:

Adequate earth ground connection of the controller is mandatory to avoid any damage or injuries.

2. Wear an ESD wrist strap, ensuring that it makes good contact with bare skin.
3. Attach the ESD wrist strap end to an earth ground (grounding screw on the back of the controller or unpainted bare metal spot of a grounded equipment rack).

4. Turn off the power switch of the controller.

 Note:

Redundant power supply units do not have a power switch.

 Warning:

The controller unit must be turned off before adding, removing, or swapping the system cards.

5. Turn off the power sources used to power the controller at the circuit breaker.
6. Disconnect all cables (except the earth ground connection) from the controller.

 CAUTION:

Power source cables must be disconnected last.

7. Unscrew the two thumb screws of the slot where you want to install or replace a card.

 Note:

Before installing a new card, refer to [About this Guide](#) on page 1.

8. Gently remove the blank plate or the existing card.
9. Gently slide the new card into the internal plastic rails of the slot.

 Note:

Insert a blank plate in each unused slot.

 Note:

While sliding in the card, take care not to damage the electronic parts on the card. The card, when properly inserted, slides in easily.

10. Tighten the thumb screws back into place. Do not over-tighten.

3.8 Cabling

To connect cables:

1. Wear an ESD wrist strap, ensuring it makes good contact with your bare skin.
2. Attach the ESD wrist strap end to an earth ground (unpainted bare metal spot of a grounded equipment rack).
3. Turn off the power switch of the controller.

Note:

Redundant Power Supply units do not have a power switch.

4. Make sure the circuit breakers of AC power sources used to power the EX Controller are off.
5. Make sure the provided power cable is connected to the EX Controller and in an appropriate AC electrical outlet.
6. Connect faxes, phones or a PBX to the FXS card.
7. Connect a PBX or ISDN line to the PRI card.
8. Connect a PSTN or a PBX to the FXO card.

This chapter contains the following sections:

- [Overview](#)
- [Prerequisites](#)
- [Accessing the EX Controller Deployment Tool](#)
- [Updating the EX Controller Deployment Tool](#)
- [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#)
- [Post-Installation Tasks](#)
- [Enabling the VNC Capability](#)

4.1 Overview

The following procedures that must be performed sequentially to complete the software installation:

1. [Accessing the EX Controller Deployment Tool](#) on page 31
2. [Updating the EX Controller Deployment Tool](#) on page 32
3. [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#) on page 34
4. [Post-Installation Tasks](#) on page 42

Note: As the EX controller does not support 802.1Q VLAN Trunks, the EX controller does not set an 802.1p Ethernet priority. The EX controller will use DSCP information to provide priority information in packets sent at layer 3. However, Ethernet Priority information and VLAN assignment must be configured at the first access port of the Ethernet switch because data will be assigned to an untagged VLAN, which is usually VLAN 1. Voice can be prioritized using the DSCP value, which can also be used to identify the Ethernet priority value set in the DSCP to Priority map in the Ethernet switch. This is also known as QoS to CoS mapping. For more details, contact your LAN switch vendor. For more examples, refer to the [MiVoice Business Engineering Guidelines](#).

4.1.1 PC Requirements

The following lists the PC requirements for the deployment:

- Windows operating system
 - Windows 11, Windows 10, Windows Vista (Business or Ultimate), Windows 8 or 8.1
 - Minimum 4 GB RAM for Windows 11 and Windows 10; Minimum 2 GB RAM for Windows Vista (Business or Ultimate), Windows 8 or 8.1

i Note: Support for Microsoft Windows Versions 8 and 8.1 ended on January, 2023. It is recommended that you upgrade to a Windows 11 Version to continue to receive security updates from Microsoft.

- Minimum 4 GB free disk space
- JRE (Java Run-time Environment) 1.6.0_1 or later installed.
- Google Chrome, Edge, or Mozilla Firefox installed.
- Latest version of UltraVNC Viewer application installed.

4.2 Prerequisites

- Download the latest **exdeploy-x.x.x.x.zip** file from **Mitel MiAccess > Software Download Center** to your deployment PC.
- Download the EX MiVoice Business software image zip file (**MiVB-9.x.x.x-yy.img.zip**) from **Mitel MiAccess > Software Download Center** to your deployment PC.
- Download the latest Mitel Configuration Wizard (MiCW) executable file (**MICW_7_x_x_x_x_Setup.exe**) from **Mitel MiAccess > Software Download Center** to your deployment PC.
- For the Mitel EX Controller MiVoice Business solution, each of the three components requires a distinct IP address.
 - EX Controller IP address:
 - Eth2-5 have a default static IP address: 192.168.0.10
 - During the deployment process outlined below, it is possible that this IP address can be altered.
 - The IP address for the "host" EX Controller must be unique.
 - Deployment Tool IP address:
 - The deployment tool is a virtual machine hosted in the EX Controller
 - By default, the virtual machine is currently set to obtain an IP address through DHCP.
 - If the DHCP is not available, the IP address of the deployment tool can be manually set either through static configuration or by utilizing a USB flash drive with a pre-configured `lan.cfg` file. Further information on both options is provided in detail later within the document.
 - The virtual machine is exclusively used for the initial deployment and is powered down and inactive thereafter. As a result, the IP address will only be necessary during the deployment process. Nevertheless, it should be a unique IP address.
 - MiVoice Business call server IP address:
 - This is a virtual machine hosted in the EX Controller.
 - The deployment tool process generates and installs this virtual machine.
 - The deployment tool, which is outlined in detail below, assigns the IP address to the MiVoice Business virtual machine.
 - The IP address for the MiVoice Business must be unique.

4.3 Accessing the EX Controller Deployment Tool

When you connect the EX Controller to a network, the Deployment Tool broadcasts its FQDN `http://exdeploy` to its local subnet through NetBIOS and acquires an IP address from the DHCP server. When the Deployment Tool successfully acquires an IP address, you can access the Deployment Tool using its FQDN `http://exdeploy`.



Warning:

Make sure that you turn on and connect only one EX Controller to the network. If you connect more than one EX Controller to the network, then you might not know which controller you are connected to.



Note: Before you run the deployment tool, you must enable VNC. To enable VNC, see the [Enabling the VNC Capability](#) section.

To access the Deployment Tool:

1. Enable NetBIOS over TCP/IPv4 on your deployment PC.
2. Ensure that the PC and the EX Controller are connected to the same subnet.
3. Connect an RJ45 Ethernet cable from any one of the **ETH2 - ETH5** ports of the EX Controller to the Layer2 switch on the network.
4. Turn on the EX Controller.

5. Enter **http://exdeploy** in the address bar of your web browser (recommended Mozilla Firefox and Google Chrome) to access the Deployment Tool.

Note: This method only works if NetBIOS has been enabled on both the PC and the network. However, some PCs are locked down, preventing this feature from being enabled. This process also requires the EX Controller to be running when a DHCP server is available to service the DHCP request from the deployment tool.

If there is no DHCP server available or NetBIOS is not running on the network, then you must manually assign a static IP address of the exdeploy VM. For more information, see [Appendix A: Assigning a Static IP Address to the EX Controller Deployment Tool](#) on page 87.

The EX Controller Deployment Tool home page is displayed.

Note: The **USB** list is available with Deployment Tool versions 1.1.13 and later. To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#) on page 105.

6. Continue with [Updating the EX Controller Deployment Tool](#) on page 32.

4.4 Updating the EX Controller Deployment Tool

After you access the Deployment Tool, you must update the Deployment Tool.

To update the Deployment Tool:

1. In the Deployment Tool home page, click **Update**.

Note:

- Updating the Deployment Tool upgrades the DGW firmware also.
- When the deployment tool is updating the EX platform with DGW firmware version 48.4 and previous versions, the Admin account password (one-time) is copied to the Snmp.SnmpV3Password parameter. However, if the DGW firmware version on the EX platform is 49.3 and later versions, a one-time password will not be triggered.

Platform variant

Call Manager type: MIVB

Call Manager image: Choose File No file chosen

USB:

General Settings

ARID: 42226718

Call Manager FQDN: ex41.vlab.local

Distinguished name: cn=ex41, ou=R&D, o=Mitel, l=Kanata, st=Ontario, c=CA

IPv4 DNS servers: 10.44.17.11, 10.44.17.31

IPv4 trusted network address: 10.0.0.0/8

Restore via console: ☐

Enable secure EX Controller access: ☐

Note: The **USB** list is available with Deployment Tool versions 1.1.13 and later. To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#) on page 105.

2. Do either of the following:

Deployment Tool Update

The deployment tool's updates are delivered as ZIP files, named `exdeploy.zip`. However you may specify other update artifacts here, particularly the EX controller firmware updates (*.bin files). Please specify the location for the update artifacts using one of the options below then click on *Check for updates*.

Upload update artifact to server No file chosen

Update using artifact from USB

Download update artifacts from URL

- Click **Choose File**, and select the **exdeploy-x.x.x.x.zip** file.
- In the **Update using artifact from USB** list, select the **exdeploy-x.x.x.x.zip** file.

Note: The **Update using artifact from USB** list is available with Deployment the Tool versions 1.1.13 and later. To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#) on page 105.

3. Click **Check for updates**.

If an update is available, the system updates the Deployment Tool. The **Progress** window displays the progress of the update. Verify the update by checking the version number displayed on the top-right corner of the Deployment Tool home page.

4.5 Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine

After you update the Deployment Tool, use the Deployment Tool to install the MiVoice Business system software as a virtual machine on the EX Controller.

Note: If the deployment fails due to interruptions, such as a power or network outage, you must restart the deployment procedure.

The Deployment Tool supports two modes of deployment to complete the installation, **Full** and **Partial + Finish**.

Full deploy

The *full deployment mode* allows you to deploy the MiVoice Business system software in a single procedure. After a full deployment, the controller starts the MiVoice Business virtual machine and shuts down the Deployment Tool virtual machine.

Partial + Full deploy

The *partial + finish deployment mode* allows you to complete the deployment in two phases.

In the first phase, the EX Controller is partially deployed. That is, after a partial deployment, the Deployment Tool virtual machine continues to run, and the MiVoice Business virtual machine is shut down. Partial deployment allows you to review and modify certain configuration parameters before you finish the deployment later.

In the second phase, you can review and modify certain configuration parameters, and then finish the deployment.

After you finish the deployment, the controller starts the MiVoice Business virtual machine and shuts down the Deployment Tool virtual machine.

To run the EX Controller Deployment Tool to install the MiVoice Business virtual machine:

1. Under **Platform Variant**, in the **Call manager** list, select **MiVB**.

Platform variant

Call Manager type: MiVB

Call Manager image: Choose File No file chosen

USB:

General Settings

ARID: 42226718

Call Manager FQDN: ex41.vlab.local

Distinguished name: cn=ex41, ou=R&D, o=Mitel, l=Kanata, st=Ontario, c=CA

IPv4 DNS servers: 10.44.17.11, 10.44.17.31

IPv4 trusted network address: 10.0.0.0/8

Restore via console: ☐

Enable secure EX Controller access: ☐

2. Do either of the following:

- If you have the **MiVB-9.x.x.x-yy.img.zip** file on your local PC, click **Choose File**, and select the **MiVB-9.x.x.x-yy.img.zip** file.
- In the **USB** list, select the MiVB-9.x.x.x-yy.img.zip file.

Note: The **USB** list is available with the Deployment Tool version 1.1.13 or later. The EX Controllers procured in MiVoice Business Release 9.2 or later have the Deployment Tool version 1.1.13 pre-installed. For more information on how to use the **USB** list, see [Assigning a static IP address by using a USB flash drive](#) on page 95. To enable the **USB** list for older systems upgraded to Deployment Tool version 1.1.13 or later, see [Appendix C: Enabling USB Ports for the Deployment Tool](#) on page 105.

3. Under **General Settings**, enter the following details:

- **ARID** — The Application Record ID (ARID) for the MiVoice Business system to acquire and register licenses with Mitel Licenses & Services. Optionally, you can license the system after the deployment through Server Manager.
- **Call Manager FQDN** — The FQDN of the MiVoice Business virtual machine. For example, coyote.acme.com, where **coyote** is the hostname and **acme.com** is the domain name (resolvable by the DNS server listed below)
- **Distinguished name** — The Distinguished Name (DN) of the MiVoice Business virtual instance that is used to create a host certificate for the controller. For example, cn= coyote, ou= Research and Development, o= Acme Company, l= Bangor, st= Maine, c= US. Leave the field as is.

Note: The hostname of the MiVoice Business system specified in the **Call Manager FQDN** field must match the cn of the **Distinguished Name** field for the certificate generated during the deployment.

- **IPv4 DNS servers** — The IP address of one or more DNS servers of the network where the EX Controller is installed; comma-separated in case of multiple DNS servers.
 - **IPv4 trusted network address** — The IPv4 address of the management networks or trusted networks from which you want to allow access to the MiVoice Business System Administration Tool and the Server Manager by generating a certificate for HTTPS use.
4. (Optional) Select the **Restore via console** check box, if you want to enable restore via server console option after the deployment. The Server Manager prompts the user to restore the system configuration upon startup.

Note: The controller does not support the **Restore from another running server** option.

5. Select **Enable secure EX controller access** to disable the SNMP v2 protocol on the EX Controller. This blocks unsecure access to the controller.

It is recommended to leave the check box cleared to configure the MiVoice Business system using the Mitel Configuration Wizard (MiCW) post deployment.

6. Optional: Select the **Enable IPv6** checkbox to enable IPv6 address.

Note: The **IPv4 default LAN gateway**, **IPv6 Call Manager LAN address**, and **IPv6 default LAN gateway** fields are visible after you enable this checkbox.

General Settings

ARID

Call Manager FQDN

Distinguished name

IPv4 DNS servers

IPv4 trusted network address

Restore via console ☐

Enable secure EX Controller access ☐

Enable IPv6 ☐

LAN Settings

IPv4 EX Controller LAN address

IPv4 Call Manager LAN address

IPv4 default LAN gateway

Figure 1: Enable IPv6 Checkbox

7. Leave the following **WAN Settings** blank unless you are setting up a WAN configuration for the EX Controller:

The screenshot displays a configuration window with two main sections: **WAN Settings** and **LAN Settings**. Each section contains three input fields. The WAN section has empty fields with placeholder text, while the LAN section has fields containing specific IP addresses. At the bottom, there is a dark blue bar with three buttons: 'Full deploy', 'Partial deploy', and 'Finish deploy'.

Section	Field Label	Value / Placeholder
WAN Settings	IPv4 EX Controller WAN address	Enter an IPv4 address/CIDR
	IPv4 Call Manager WAN address	Enter an IPv4 address
	IPv4 default WAN gateway	Enter an IPv4 address
LAN Settings	IPv4 EX Controller LAN address	10.37.27.60/24
	IPv4 Call Manager LAN address	10.37.27.61
	IPv4 default LAN gateway	10.37.27.1

Full deploy | Partial deploy + Finish deploy

- a. IPv4 EX Controller WAN address
- b. IPv4 Call Manager WAN address
- c. IPv4 default WAN gateway

8. Under **LAN Settings**, specify the IPv4 and IPv6 LAN settings:

- a. **IPv4 EX Controller LAN address** — IPv4 address with CIDR for the EX Controller Web GUI that will overwrite the default IP address of the EX Controller Web GUI. For example, 10.211.13.42/12.
- b. **IPv4 Call Manager LAN address** — IPv4 address for the MiVoice Business system virtual machine. (No CIDR is required)
- c. **IPv4 default LAN gateway** — IPv4 default LAN gateway address
- d. **IPv6 EX Controller LAN address** — IPv6 address with CIDR for the EX Controller Web GUI that will overwrite the default IP address of the EX Controller Web GUI. For example, 2023:f:b:2251::196/128.
- e. **IPv6 Call Manager LAN address** — IPv6 address for the MiVoice Business system virtual machine. (No CIDR is required)
- f. **IPv6 default LAN gateway** — IPv6 address with CIDR for the EX Controller Web GUI that will overwrite the default IP address of the EX Controller Web GUI. For example, 2023:f:b:2251::1

LAN Settings

IPv4 EX Controller LAN
address

Enter an IPv4 address/CIDR

IPv4 Call Manager LAN
address

Enter an IPv4 address

IPv4 default LAN gateway

Enter an IPv4 address

IPv6 EX Controller LAN
address

Enter an IPv6 address/Prefix Length

IPv6 Call Manager LAN
address

Enter an IPv6 address/Prefix Length

IPv6 default LAN gateway

Enter an IPv6 address/Prefix Length

9. If you want to perform a **partial + finish** deploy, skip this step and proceed to step 10. If you want to deploy and enable the MiVoice Business virtual machine immediately, click **Full deploy**.

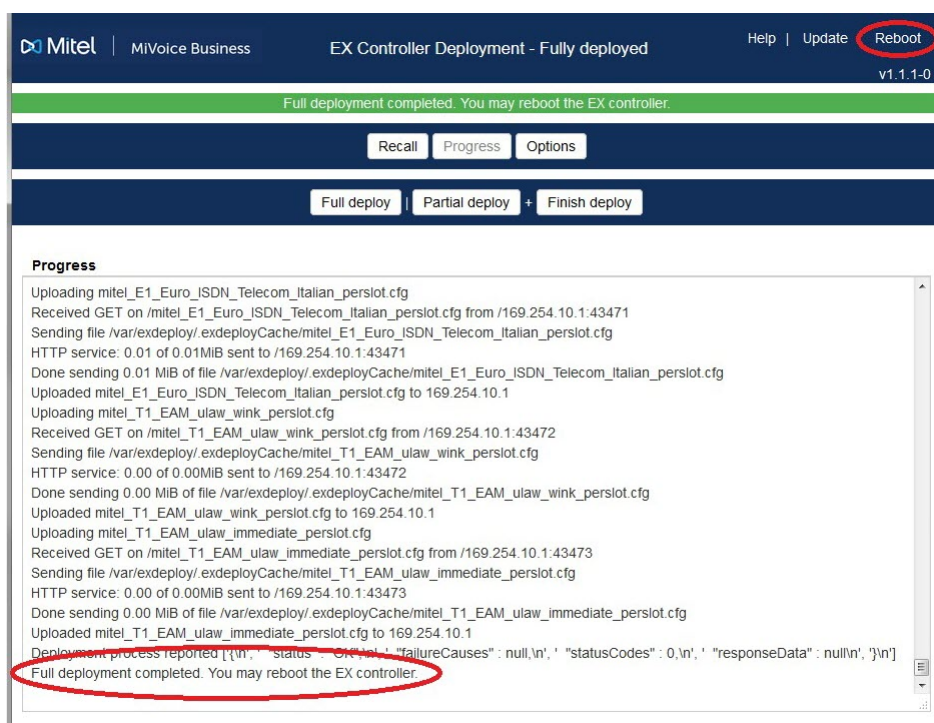
A confirmation message is displayed.

- a. Click **OK** to confirm the deployment.

Note: Ignore the warning message about FQDN. For example, “FQDN coyote.acme.com is not resolvable”.

The system starts the full deployment process. It takes approximately 25 minutes to complete the deployment. When the deployment is complete, the following message is displayed.

“Full deployment completed. You may reboot the EX controller.”



- b. Continue with [step 11](#).

10. If you want to deploy now but configure and enable the MiVoice Business virtual machine later, click **Partial deploy**.

A confirmation message is displayed.

- a. Click **OK** to confirm the deployment.

i Note: Ignore the warning message about FQDN. For example, "FQDN coyote.acme.com is not resolvable".

The system starts the partial deployment process. It takes approximately 25 minutes to complete the deployment.

- b. After the partial deployment, if required, power off the EX Controller, and finish the deployment later.
- c. When you want to enable the MiVoice Business virtual machine, [access the Deployment Tool](#). If you have already accessed the Deployment Tool, continue with the next step.
- d. If required, click **Recall** to go back to the Deployment Tool home page to review and modify **General Settings**, **WAN Settings**, and **LAN Settings**.

i Note:

You can modify only **General Settings**, **WAN Settings**, and **LAN Settings**. Other configuration parameters are blocked for modification.

- e. Click **Finish deploy**.

A confirmation message is displayed.

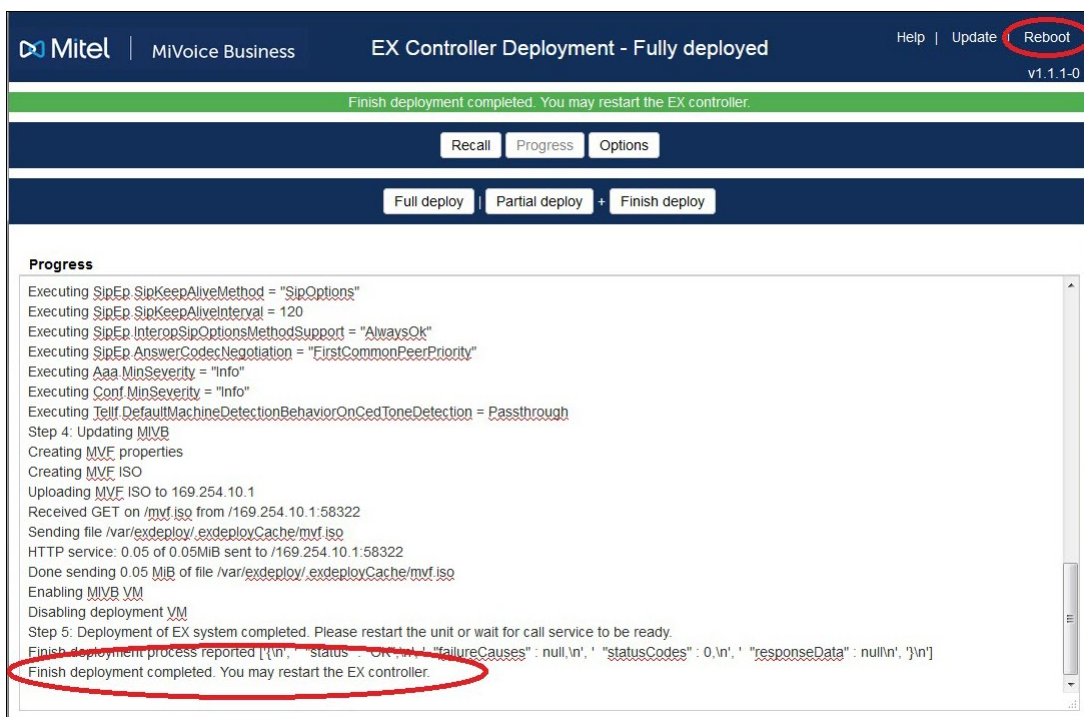
- f. Click **OK** to confirm the deployment.

i Note: Ignore the warning message "FQDN coyote.acme.com is not resolvable".

The system starts to finish the deployment. It takes approximately 2 minutes to finish the deployment.

- g. When the deployment is complete, the following message is displayed.

"Finish Deployment Completed. You may restart the EX controller."



h. Continue with [step 11](#).

11. Click **Reboot** to restart the EX Controller.

It takes approximately 20 minutes for the EX Controller to boot the first time. Subsequent reboots are faster.

After the reboot, the Deployment Tool virtual machine shuts down and MiVoice Business virtual machine starts automatically.

12. Ensure that you have the system on the correct network for the new IP addresses as configured during the deployment process.
13. If you have inserted the USB flash drive, remove the USB flash drive from the EX Controller.

Note: The 'Image and Text Notification' feature in the Revolution Server is not functional on IPv6-registered phones. This feature works as expected on IPv4-registered phones.

4.6 Post-Installation Tasks

4.6.1 Default Passwords

The default user names and passwords to be used after the deployment are as follows:

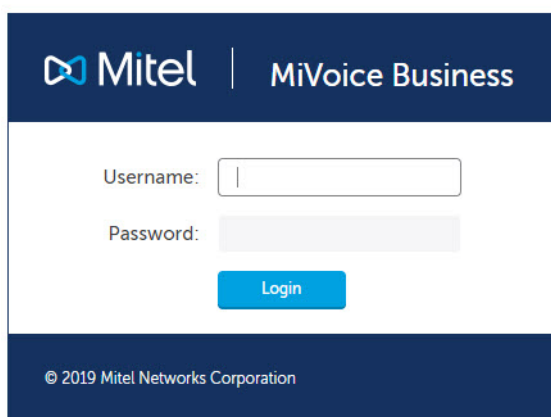
- The default user name for the Server Manager user accounts is **admin** and **root** and the default password is **default1**.

- The default user name for the System Administration Tool user account is **system** and the default password is **password**.
- The default user name for the EX Controller Web GUI user account is **public**. There is no default password.

4.6.2 Log into Server Manager

1. Log into Server Manager by entering **<IP (IPv4 or IPv6) Call Manager LAN address>/server-manager** in the address bar of your web browser.

The Server Manager login page is displayed.



2. Type the default **Username** (admin) and **Password** (default1).

You are prompted to change the password. The new password must have at least eight characters consisting of:

- an upper case letter
- a lower case letter
- a number
- a non-alphanumeric character

For more information on password quality requirements, refer to the Help page associated with the Password Requirements tab in the Administration > System users page on Server Manager.

Note: The modified password is also applied as the SNMP v3 privacy password, the EX Controller Web GUI password, and the System Administration Tool mimx account password. However, if the new password does not conform with the minimum eight-character rule, it does not get synchronized. For information about troubleshooting the password synchronization issue, see [Unable to log into the EX Controller Web GUI as mimx user after a password reset using Server Manager](#).

4.6.3 Licensing the MiVoice Business system

If you did not specify the ARID during the deployment, license the MiVoice Business system using Server Manager (**ServiceLink > Status**).

1. [Log into Server Manager](#) on page 43.
2. Navigate to **ServiceLink > Status**.
3. In the **Service account ID** field, enter the Application Record ID (also called Service account ID).
4. If the Internet is accessed via a proxy, enter:
 - Address of proxy
 - TCP port used to connect to proxy. The proxy server must be configured to forward TCP packets on the incoming port to the License Server address (sync.mitel-amc.com) on port 22.
5. Click **Activate** to synchronize with Licenses & Services and activate ServiceLink.

Following successful activation, Server Manager periodically reconnects to the Licenses & Services (every 24 hours by default) via a secure, encrypted connection to synchronize ServiceLink status information. New configuration instructions, such as services you have added or deleted to your Licenses & Services account, are updated at this time.

4.6.4 Log into the MiVoice Business System Administration Tool

1. Log into the MiVoice Business System Administration Tool by entering **<IP (IPv4 or IPv6) Call Manager LAN address>** in the address bar of your web browser.

The System Administration Tool login page is displayed.

Mitel | MiVoice Business

Login ID

Password

☐ Remember Login ID

Login

[Install MiVoice Business Certificate](#)

[Enable pop-ups](#)

2. The first time you connect, you must install the MiVoice Business certificate.

Chrome and Edge

To install the MiVoice Business certificate:

- a. On the login page, click **Install MiVoice Business Certificate** and follow the instructions provided to install the certificate.

Firefox

To install the MiVoice Business certificate:

- a. Start a System Administration Tool session by connecting to the MiVoice Business system.
- b. Click **I Understand the Risks** followed by **Add Exception...**
- c. Clear the **Permanently store this exception** check box, and then click **Confirm Security Exception**.
- d. Once you confirm the exception, the System Administration Tool Login page will be displayed.

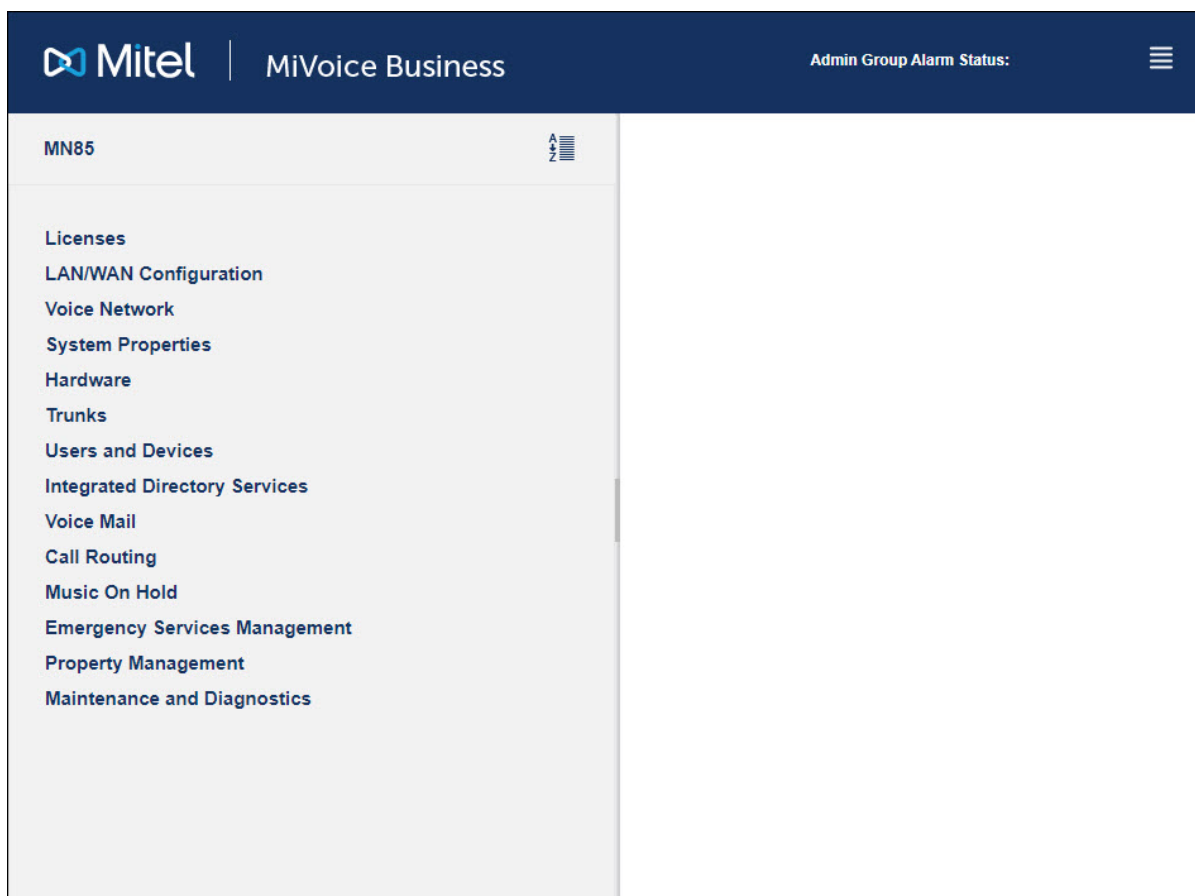
Click **Install MiVoice Business Certificate** and follow instructions provided to install the certificate. After the certificate is installed, exit the browser, and then restart it. You can now log in to MiVoice Business and not receive the security certificate warnings.

3. Type the default **Login ID** (system) and **Password** (password).
4. Select **Remember Login ID** if you want to save the Login ID on your computer.
5. Click **Log In**.

To prevent unauthorized use, you will be prompted to change the password the first time you log in.

6. Click **System Administration Tool**.

The System Administration Tool home page is displayed.



7. You will be prompted to install XML Components when you log into the System Administration Tool for the first time. At the prompt, “Do you wish to install or upgrade the required XML components?”, click **Install Now**. The installation takes less than 30 seconds and you do not need to restart your computer.

Note: The system allows up to 5 concurrent System Administration Tool or Group Administration Tool sessions (or any combination of the two) provided that the initial login browser is closed and 10 concurrent Desktop Tool sessions.

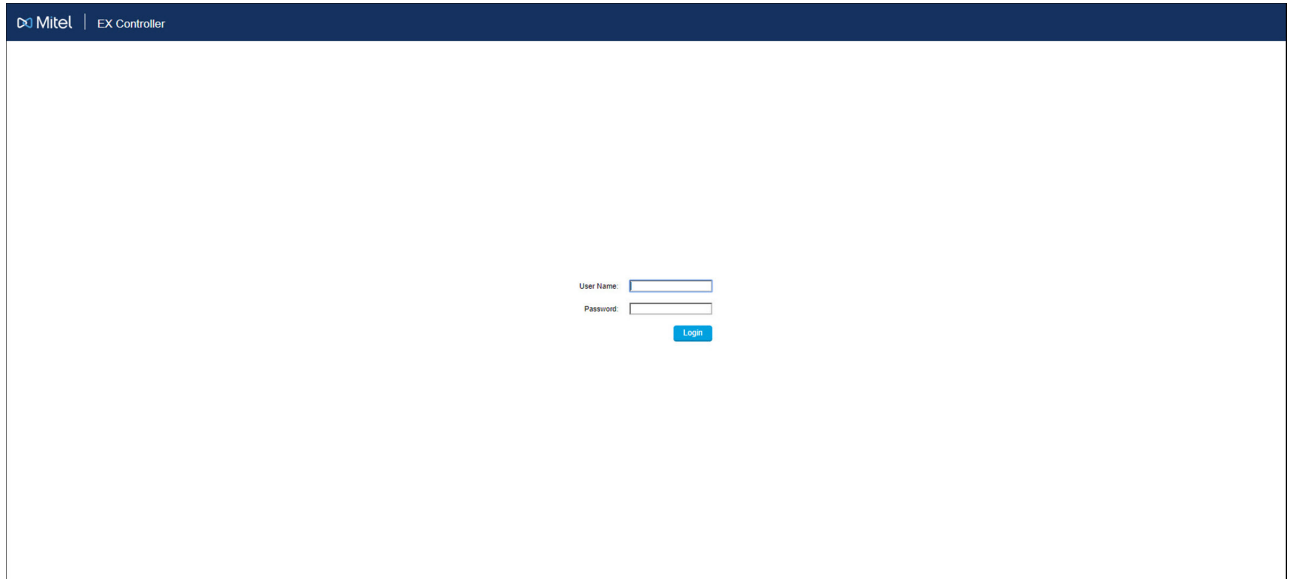
Note: The System Administration Tool will temporarily lock you out for 15 minutes after three consecutive attempts to log in have failed.

8. Navigate to the **Hardware > Hardware Modules** form and verify that all the telephony cards are listed.
9. Reboot the system from Server Manager (**Administration > Shutdown or reboot**).

4.6.5 Log in to the EX Controller Web GUI

1. Enter the **IP (IPv4 or IPv6) EX Controller LAN address** specified during the deployment in the address bar of your web browser.

The EX Controller Web GUI login page is displayed.



The screenshot shows the login page of the Mitel EX Controller Web GUI. At the top, there is a dark blue header bar containing the Mitel logo and the text 'EX Controller'. The main content area is white and features a login form centered on the page. The form consists of two input fields: 'User Name' and 'Password', each with a small blue border. Below the 'Password' field is a blue button with the word 'Login' in white text.

2. In the **User Name** field, type **public**.
3. In the **Password** field, type the password of the Server Manager's **admin** user.

4. Click **Login**.

The EX Controller Web GUI home page is displayed.

Current Status	
Device Identification:	EX Controller
Firmware:	Dgw 44.3.1746
Profile:	STNL-MT-D2000-155
MAC Address:	0090f80bdc88
Serial Number:	000400001M318170017
Number of DSPs:	0
Storage Memory (in use/total):	18.3 GB / 60 GB
Volatile Memory (in use/total):	2.3 GB / 8 GB
System Uptime (D:HH:MM:SS):	12:19:04:19
System Time (DD/MM/YYYY HH:MM:SS):	28/11/2019 02:34:15

Licences	
CWMP/TR-069	
SBC Licence for 3 concurrent sessions	
Virtual Machine Licence	

Activate Licence	
Licence Key:	

If the login fails, see [Unable to log into the EX Controller Web GUI as mimx user after a password reset using Server Manager](#).

Important:

The EX Controller Web GUI is used for troubleshooting purposes only. Do **NOT** use this GUI for programming trunks or the MiVoice Business system. Use the MiVoice Business System Administration Tool for programming trunks (**Trunks > Enterprise Gateways**) and the MiVoice Business system.

4.6.6 Program the MiVoice Business System

1. Program the MiVoice Business system using one of the following options:

- Mitel Integrated Configuration Wizard (only if you have cleared the **Enable secure EX controller access** check box (step 6) in the [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#) on page 34)
- Manually, by logging into the MiVoice Business System Administration Tool

2. (Optional) If you are migrating from an unsupported 3300 ICP controller, continue with step 6 of the **Migration Guidelines for an Unsupported 3300 ICP Controller** procedure (**Chapter 4 Migration**) in the *MiVoice Business Migration Guidelines* document.

4.6.7 Trunk Configuration

After you perform the basic programming of the MiVoice Business System Administration Tool, you can configure trunks automatically by executing configuration scripts in the **Gateway Configuration Scripts** form (**Trunks > Enterprise Gateways**) of the MiVoice Business System Administration Tool.

Note: On the EX platform, individual trunk access is not supported as ISDN, T1, and FXO trunks are not assigned trunk numbers when programmed.

Note:

If you hover over the default configuration file, a Tooltip is displayed that provides information about the default configuration file.

Trunk	Configuration Details
T1/D4 E&M trunks	Execute the following configuration scripts: - To configure Immediate Start, execute: <code>mitel_T1_EAM_ulaw_immediate_perslot.cfg</code> - To configure Wink Start, execute: <code>mitel_T1_EAM_ulaw_wink_perslot.cfg</code>
PRI trunks	Execute one of the following configuration scripts depending on the protocol provided by the PSTN: <code>mitel_E1_Euro_ISDN_Euro_Cayman_perslot.cfg</code> <code>mitel_E1_Euro_ISDN_Euro_Numeris_perslot.cfg</code> <code>mitel_E1_Euro_ISDN_Euro_Standard_perslot.cfg</code> <code>mitel_E1_Euro_ISDN_Euro_Telecom_Italian_perslot.cfg</code> <code>mitel_T1_DMS100_perslot.cfg</code> <code>mitel_T1_DMS250_perslot.cfg</code>

Trunk	Configuration Details
FXO trunk	Execute the following configuration scripts: - To configure FXO trunks that use loaded coils, execute: <code>mitel_fxo_north_america.cfg</code> - To configure FXO trunks that use non-loaded coils, execute: <code>mitel_fxo_default.cfg</code> - To disable the Dial Tone Detection Mode, execute: <code>mitel_Disable_Dialtone_Detection.cfg</code>
R2 trunk	To configure R2 trunks, execute the configuration file applicable to your country: - To configure R2 trunks execute: <code>mitel_R2_Argentina_perslot.cfg</code> <code>mitel_R2_Brazil_perslot.cfg</code> <code>mitel_R2_ITU_perslot.cfg</code> i Note: <code>mitel_R2_ITU_perslot.cfg</code> is applicable for generic ITU configuration. <code>mitel_R2_Mexico_perslot.cfg</code> <code>mitel_R2_Philippines_perslot.cfg</code> <code>mitel_R2_SaudiArabia_perslot.cfg</code> <code>mitel_R2_Venezuela_perslot.cfg</code> - You can also manually program the R2 trunk using the EX Controller Web GUI. For more information about Programming R2 Trunk and Customizing default settings, see Appendix B: Programming R2 Trunks on page 98

4.7 Enabling the VNC Capability

To enable VNC for the exdeploy virtual machine or MIVoice Business virtual machine:

1. [Log in to the EX Controller Web GUI](#) on page 47.
2. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

3. Click  to stop the required virtual machine
4. Do the following:

- a. For the **VM Name** field **exdeploy**, in the **VNC Id** field, enter **0**.
- b. For the **VM Name** field **MIVB**, in the **VNC Id** field, enter **1**.

 **Note:** Any value of 0 or greater enables VNC access for that VM.

5. Click **Apply** to apply the changes.
6. Click  to start the virtual machine.

 **Note:** If you enable VNC, it might open a security hole and recommend disabling it for a secure system.

Maintenance

5

This chapter contains the following sections:

- [Software Upgrade](#)
- [Backup and Restore](#)
- [Field Replaceable Units](#)
- [Change IP Address of the EX Controller Web GUI](#)
- [Configure the Server Using Server Console](#)

5.1 Software Upgrade

You can upgrade the MiVoice Business system software using the blades utility in Server Manager (**ServiceLink > Blades**).

 MiVoice Business

admin@kendallex.support.lab Status: Major

ServiceLink

Blades

Status

Administration

Web services

Backup

Restore

View log files

Event viewer

System information

System users

Shutdown or reboot

Security

Remote access

Syslog

Web Server

Configuration

Networks

E-mail settings

Google Apps

Cloud Service Provider

DHCP

Date and Time

Hostnames and addresses

Domains

IPv6-in-IPv4 Tunnel

SNMP

Ethernet Cards

Review configuration

Miscellaneous

Support and licensing

Help

EX Platform

Reboot

Current list of blades

Update list

Software download center: swdlgw.mitel.com

Last updated: Fri 10 Nov 2023 01:02:56 AM EST

Blade	Description	Status	Installation	Documentation
EX	EX Platform Specific Software	installed	installed (V2.2.0.13) <a>Upgrade <a>Cache (v2.2.0.14)	
MPA Probe (MarWatch Probe Blade)	The MPA Probe service is used with the MPA monitoring platform. It requires additional system resources on the host Virtual Machine. Ensure that adequate vCPU and memory are available before using this service. Refer to Mitel Virtual Appliance Deployment Guidelines and product Engineering and Solution Guidelines for details.		<a>Install <a>Cache (v6.5.9.32) <a>Install <a>Cache (v6.6.4.115) <a>Install <a>Cache (v6.7.1.155)	
MVF	The Mitel Virtualization Framework provides features and functions to support a Virtual Infrastructure for Mitel Applications. It also bundles VMWare Tools, wrapped to work correctly on Mitel Standard Linux.	installed	installed (V6.0.0.1) <a>Upgrade <a>Cache (v6.0.0.4) <a>Upgrade <a>Cache (v6.0.0.5) <a>Upgrade <a>Cache (v6.0.0.8)	
MiVoice Business	MiVoice Business software for installation on MVB vApp and ISS platforms.	installed	<a>Remove (v9.4.0.25) <a>Upgrade <a>Cache (v9.4.1.18) <a>View <a>Upgrade <a>Cache (v9.4.1.19) <a>View <a>Upgrade <a>Cache (v9.4.1.21) <a>View <a>Upgrade <a>Cache (v10.0.0.76) <a>View <a>Upgrade <a>Cache (v10.0.1.18) <a>View	
ServiceLink	ServiceLink for Mitel Standard Linux	installed	installed (V11.0.99.0) <a>Upgrade <a>Cache (V11.0.102.0) <a>Upgrade <a>Cache (V11.0.105.0) <a>Upgrade <a>Cache (V11.0.106.0)	

MiVoice Business 9.4.0.25
© Mitel Networks Corporation

5.1.1 Prerequisite

Ensure that the network backup is configured properly in Server Manager (**Administration > Backup**).

5.1.2 Procedure

To upgrade the software

CAUTION:

The upgrade process causes service interruption.

1. [Log into Server Manager](#) on page 43.
2. Click on **Blades**, located in the left-side panel under **ServiceLink**.
3. Click **Update List** to view the new versions available from the Licenses & Services in the blade list.
4. Install the blades in the following order:
 - a. Service Link
 - b. MVF
 - c. EX blade
 - d. MiVoice Business
5. Read the End User License Agreement, and at the bottom of the page click **Accept all Licenses**. A page showing the upgrade progress appears.
6. When the installation is complete, click **Clear this report**.

Note:

The installation time is dependent on the size of the database being backed up. The system takes approximately 10 to 20 minutes to back up an average-sized database (50 - 100 MB).

 **Note:** If you are upgrading the EX servers running MSL 11.x to MSL 12.x or later without the need for physical media or console access, follow the steps in [Upgrade with Remote Fresh Install Blade](#).

5.1.3 Upgrade with Remote Fresh Install Blade

You can upgrade EX servers running MSL 11.x to MSL 12.x or later without the need for physical media or console access. The minimum version for RFI upgrade is MiVoice Business Release 9.1.2.4 with MSL version 11.0.69.0.

Note: The RFI blade requires 5 GB of disk space for a backup. To view the hard disk (HD) space required to do the RFI upgrade, you must do the following:

1. Log into Server Manager.
2. Navigate to **Administration > System Information**.
3. In the **Information** page, under **Mounted Filesystems**, verify that the value in the **Free** field is more than 5 GB. See [System Information](#) for more information.

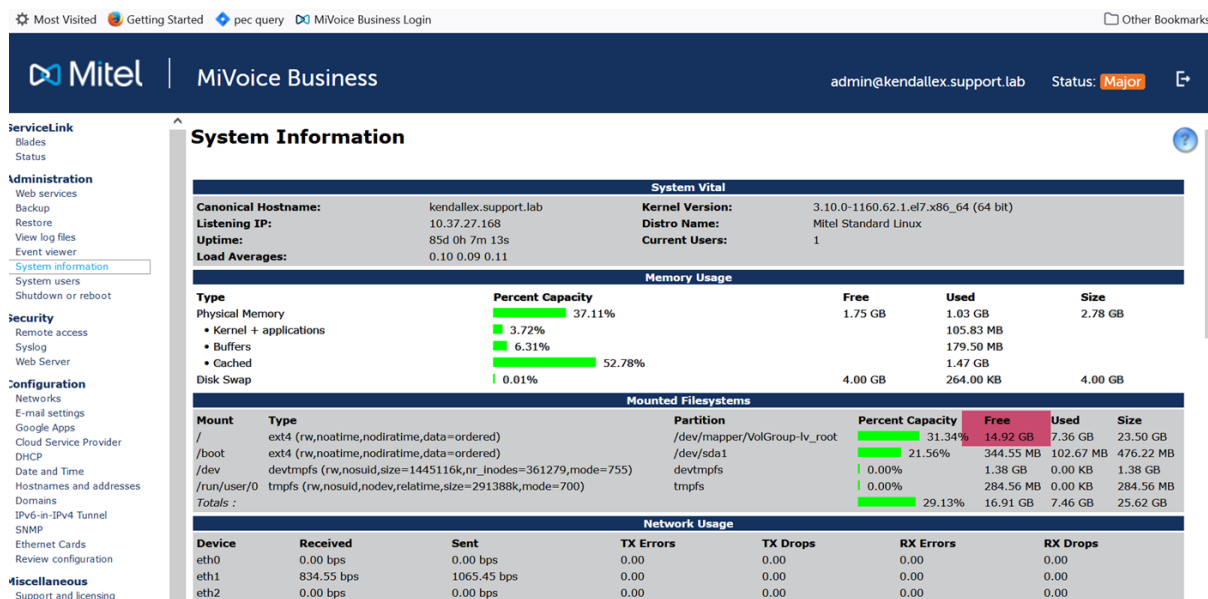


Figure 2: System Information

To perform a remote fresh install:

1. Perform a backup through the Server Manager (this step is recommended).

Note:

- See [Backup and Restore](#) for more information.
- You must note the Backup parameters. This is because if the RFI fails, this information is required when you are [Restoring an EX from a Server Manager Backup](#).



CAUTION: In the Server Manager, under **Service Link**, click **Blades**. In the **Blades** page that opens, you must take a screenshot of the installed blades for later reference. You must also capture other MSL data such as, Service Account ID, Date and Time, Network Backup, Networks, remote access, Domains and so on.

2. In the Server Manager, under **ServiceLink**, click **Blades** and then click **Update List**.
3. Locate the Remote Fresh Install blade and click **Install** link beside it.

4. Accept the software license agreements when prompted.
5. Wait for the installation to complete.

 **Note:** The RFI blade is a large file and will require approximately 5 minutes to download before installing it.

6. In the Server Manager, under **Administration**, click **Shutdown or reboot**, select **Reboot** and then click **Perform**.
7. Click **Yes** to confirm the reboot.
8. When the reboot is complete, which can take 10-15 minutes, log back in to the Server Manger and confirm the configuration data for Server Manager. Configuration data for Server Manager includes Service Account ID, Date and Time, Network Backup , Networks, remote access, and so on. If there is a problem, restore from the backup.
9. Under **ServiceLink**, click **Status** and then click **Sync** to perform a sync with the Licenses & Services.

10. Reinstall your application software. To do so:

- a. Go to **Blades Panel** and click **Update list** to see blades that can be installed.
- b. Under MVF Blade click **Install**.
- c. Click **Accept all licenses** to begin the installation.
- d. After the installation is complete, click **Clear this report**.
- e. Go to **Blades Panel** and under EX Blade click **Install**.
- f. Click **Accept all licenses** to begin the installation.

Note: After the EX Blade is installed, the firmware will be upgraded to DGW 49.1 or later versions. When the upgrade is complete, the EX platform will automatically reboot after a few minutes. You may receive a message on the page stating that the reboot will happen automatically, or the page may fail to refresh because it is already in the process of rebooting. In this situation, you must wait for 3 minutes and then refresh the browser or you might have to login to Server Manager again. An example of the firmware updated message text is as follows:

Firmware successfully updated on EX (10.37.27.98) with status **WaitingManualRestart**.
The EX platform will reboot automatically in a few minutes.
The system is ready to use after the reboot.

- g. After the installation is complete, click **Clear this report**.
- h. Go to **Blades Panel** and under MiVoice Business Blade, click **Install**.
- i. Click **Accept all licenses** to begin the installation.
- j. After the installation is complete, click **Clear this report**.
- k. Wait for few minutes for the restore of the MiVoice Business database to complete.

Note:

- You might have to refresh the page to determine whether the installation is complete.
- Clear the web browser cache after installing MiVoice Business RFI Blade.

Note: After the installation is complete, to install optional blades if required, refer to the screenshot taken in [step 1](#) before the RFI upgrade.

5.1.4 Restoring an EX from a Server Manager Backup

To restore an EX controller from a Server Manager backup, follow these steps:

1. Install the required software load using the EX deployment tool.
2. [Log into Server Manager](#) on page 43.
3. In the Server Manager, under **Administration**, click **Backup**.
4. In the **Backup server data** page that opens, under **Backup configuration and status**, select **Configure network backup** from the drop-down list.

5. In the **Network Backup** page that opens, complete all the required fields.
6. Click **Save** to validate your server configuration. If validation is successful the **Backup Now** button will appear.
7. Under **Administration**, click **Restore**.
8. In the **Restore from Network** page that opens, from the **Restore Source Type** drop-down list, select the type of network restore.
9. Complete all the required fields.
10. Click **Next**.

The system validates and lists all the database backup files available in the specified location on the network in the **Select backup file** drop-down list.

11. In the **Select backup file** drop-down list, select the database backup file you want to restore.
12. If the database backup file was encrypted when creating the backup, then enter the password in the **Encryption Password** field.
13. Click **Next**. A confirmation message is displayed.
14. Click **Yes** to restore the database. The system reboots and restores the database upon restart.

 **Note:** The **Restore from Network** page displays only the last restore status of the server.

5.1.5 Mount Software Blade on Server Manager Manually

If a software blade is not available on Licenses & Services or Server Manager for an upgrade, you can manually mount the software blade on Server Manager and then perform the software upgrade.

To manually mount the software blade on Server Manager and upgrade the software:

1. Using a file transfer application (for example, FileZilla), copy the downloaded software blade ISO file to the **tmp** folder under the *root* directory in the MiVoice Business system.
2. Using a terminal emulator application (for example, PuTTY), connect to the MiVoice Business system remotely as *root* user using the SSH protocol.
3. Run the following commands:
 - a. `cd /tmp`
 - b. `mkdir -p /mnt/cdrom`
 - c. `mount Blade-MiVoiceBusiness-9.1.0.88-01.iso /mnt/cdrom`

mount: /dev/loop0 is write-protected, mounting read-only

 - d. `cd /mnt/cdrom/Software/`
4. [Log into Server Manager](#) on page 43 and verify that the mounted software blade is displayed in the **ServiceLink > Blades** page.
5. [Perform the software upgrade](#).

6. If the remote connection with the MiVoice Business system established in step 2 is lost, perform step 2, and then run the following commands:

- a. `cd`
- b. `umount /mnt/cdrom`
- c. `rm Blade-MiVoiceBusiness-9.1.0.88-01.iso`
- d. At the following prompt, type **y**.

```
rm: remove regular file 'Blade-MiVoiceBusiness-9.1.0.88-01.iso'?
```

5.2 Backup and Restore

You can perform database backup and restore either from Server Manager or the MiVoice Business System Administration Tool.

5.2.1 Backup and Restore Using Server Manager

The database backup using Server Manager includes the server database, the EX Controller (host) database, and the MiVoice Business system database.

To perform a backup, log into the Server Manager, and navigate to **Administration > Backup**. For more information, refer to the associate Help page.

To perform a restore, log into the Server Manager, and navigate to **Administration > Restore**. For more information, refer to the associate Help page.

5.2.2 Backup and Restore Using MiVoice Business System Administration Tool

The database backup using the MiVoice Business System Administration Tool includes the MiVoice Business system database.

Note:

The database backup generated from the System Administration Tool does not include the EX Controller (host) database.

To perform a backup, log into the MiVoice Business System Administration Tool, and navigate to **Maintenance and Diagnostics > Backup**. For more information, refer to the associate Help page.

To perform a restore, log into the MiVoice Business System Administration Tool, and navigate to **Maintenance and Diagnostics > Restore**. For more information, refer to the associate Help page.

 Warning:

Do NOT restore the MiVoice Business system database on a blank EX Controller (that is, an EX Controller (host) with no database). Otherwise, there will be data inconsistency.

5.3 Field Replaceable Units

5.3.1 Cooling Fan/Power Supply/Solid State Drive

In case of failure these internal EX Controller sub-systems are not field serviceable, you must replace the EX Controller unit:

1. Make a note of the slot number and telephony card (PRI, DSP, FXO, or FXS) installed into the slot. For example, slot 1 has PRI card installed, slot 2 has DSP card installed, and so on.
2. Ensure that you have the latest backup file from Server Manager.
3. Remove the telephony cards from the EX Controller. See [Telephony Cards](#) on page 59.
4. Procure a new EX Controller. For part numbers, see [Models and Part Numbers](#) on page 12.
5. Install the EX Controller. See [Hardware Installation](#) on page 19.

 Note:

Ensure that you install the cards in the slots as noted in step 1.

6. Deploy the system software. See [Software Installation](#) on page 29.

Ensure to select the **Restore via console** option in the EX Controller Deployment Tool.

7. Restore the database from the Server Manager (**Administration > Restore**).

5.3.2 Telephony Cards

If you are replacing a card, it is recommended to replace a card with the same type of card in a slot. For example, replace an FXO card with a new FXO card. If you replace a card with a different type of card or move a card to a different slot, then the configuration data is lost. You must deprogram the old card and reprogram the new card.

Current slot configuration	If the new card you want to install is	Recommended action
Slot 1 - PRI	PRI	1. Replace the DSP card in slot 2 with the PRI card. 2. Install the DSP card in slot 5 (next available slot).
Slot 2 - DSP		
Slot 3 - FXO	DSP	Install the DSP card in slot 5 (next available slot).
Slot 4 - FXS		
	FXO or FXS	Install the FXS or FXO card in slot 5 (next available slot).
Slot 1- DSP	PRI	1. Replace the DSP card in slot 1with the PRI card. 2. Install the DSP card in slot 4(next available slot).
Slot 2- FXO		
Slot 3- FXS	DSP	Install the DSP card in slot 4 (next available slot).
	FXO or FXS	Install the FXS or FXO card in slot 4 (next available slot).

To add or replace a card:

1. Make sure an adequate earth ground connection has been made between the grounding screw on the back of the controller and an appropriate grounding point in your site.



Warning:

Adequate earth ground connection of the controller is mandatory to avoid any damage or injuries.

2. Wear an ESD wrist strap, ensuring that it makes good contact with bare skin.
3. Attach the ESD wrist strap end to an earth ground (grounding screw on the back of the controller or unpainted bare metal spot of a grounded equipment rack).

4. Turn off the power switch of the controller.

 Note:

Redundant Power Supply units do not have a power switch.

 Warning:

The controller unit must be turned off before adding, removing or swapping cards.

5. Disconnect all cables (except the earth ground connection) from the controller.

 CAUTION:

Power source cables must be disconnected last.

6. Unscrew the two thumb screws of the slot where you wish to install or replace a card.
7. Gently remove the blank plate or the existing card.
8. Gently slide the new card into the internal plastic rails of the slot.

 Note:

The slot must not be left empty. If do not want to install a new card after removing a telephony card, insert the blank plate in the slot.

 Note:

While sliding in the card, take care not to damage the electronic parts on the card. The card, when properly inserted, slides in easily.

9. Set the thumb screws back into place. Do not over-tighten.
10. Apply the label indicating the ISED and ACTA registration numbers on the exterior surface of the casing.

5.4 Change IP Address of the EX Controller Web GUI

To change IP address of the EX Controller Web GUI (EX Controller):

Note:

Do not change the IP address from the EX Controller Web GUI.

1. To change the IP address of the host Mitel EX Platform:

- a. Log in to the System Administration Tool.
- b. Navigate to the **Voice Networks > Enterprise Gateways** form.
- c. Click the Current IP address to get the host Mitel EX platform.
- d. Click **Change**.
- e. Enter the new IP scheme in the three advanced fields:

i. **Update IPv4 Address**

ii. **Update IPv4 Subnet Mask**

iii. **Update IPv4 Gateway Address**

f. Click **Save**.

Enterprise Gateways on **ex207** Search DN ▼

Add **Change** **Delete**

Enterprise Gateways

IP/FQDN
10.211.26.205

Change

Enterprise Gateways

IP/FQDN 10.211.26.205

Authentication

Privacy Password

User mimx

Password

Advanced

Update IPv4 Address

Update IPv4 Subnet Mask

Update IPv4 Gateway Address

Save **Cancel**

Figure 3: Enterprise Gateway form

2. To change the virtual MiVB running on the Mitel EX:
 - a. Connect with putty to the current MiVB IP In SSH mode to port 22
 - b. Login as: admin
 - c. Password: your MSL server manager password
 - d. Choose option 2 **configure this server**
 - e. Make the required changes to the IP config.

Note: Mitel does not recommend making any changes or modifications in the Mitel EX interface unless specifically directed.

Ensure that the EX Controller and the MiVoice Business system are on the same subnet. If the EX Controller is on a different subset, then [Change the IP address of the MiVoice Business system](#) to the same subnet as that of the EX Controller.

5.5 Configure the Server Using Server Console

The server console provides basic, direct access to the server. Most server console operations are also available from the server manager. You can also perform basic MSL configuration using the Server Console.

5.5.1 Accessing Server Console

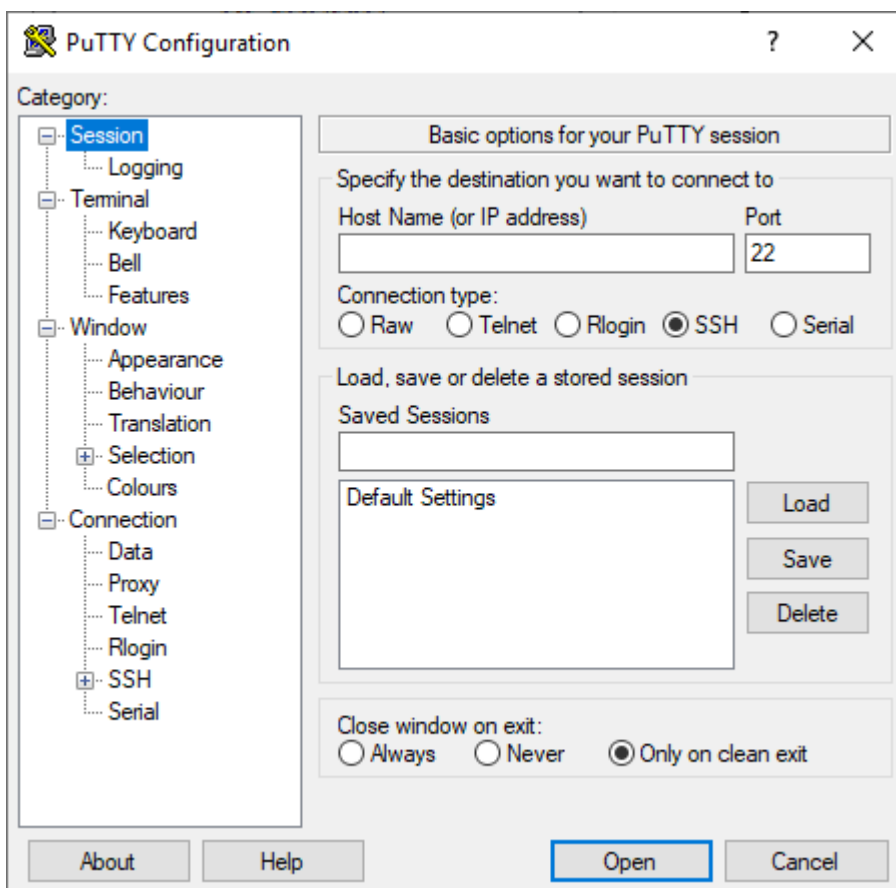
To access the Server Console remotely:

1. Connect to the MiVoice Business system using a terminal emulator application (for example, PuTTY).

Note:

Before you begin, ensure that you have enabled SSH access through the Server Manager (**Security > Remote Access**).

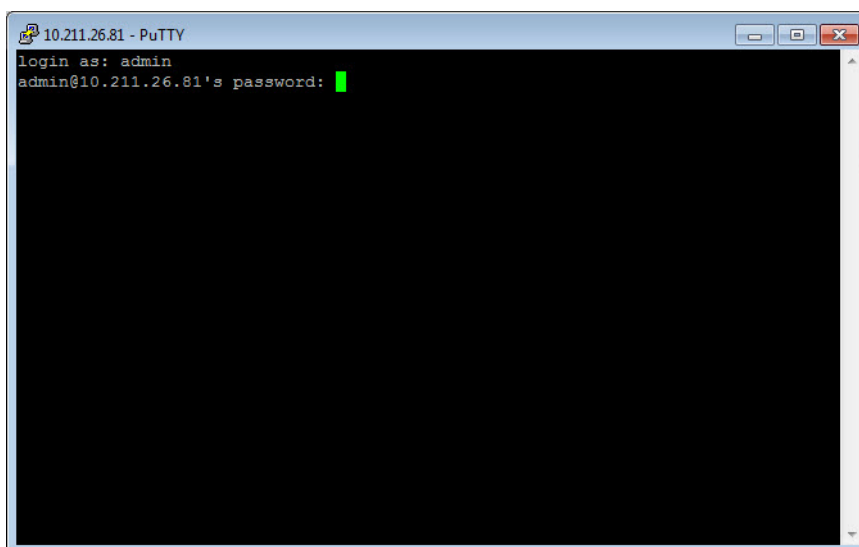
- a. Launch a terminal emulator application.



- b. In the **Host Name (or IP address)** field, type the IP address of the MiVoice Business system.
- c. Select **SSH** under **Connection** type, and then click **Open**.

The login prompt is displayed.

- d. At the login prompt (**login as:**), type **admin** (user *admin*) and press the Enter key.



Note:

You can also log in as the *root* user and type **su admin** to switch to the *admin* user.

- e. At the password prompt, type the administrator password, and press the ENTER key.

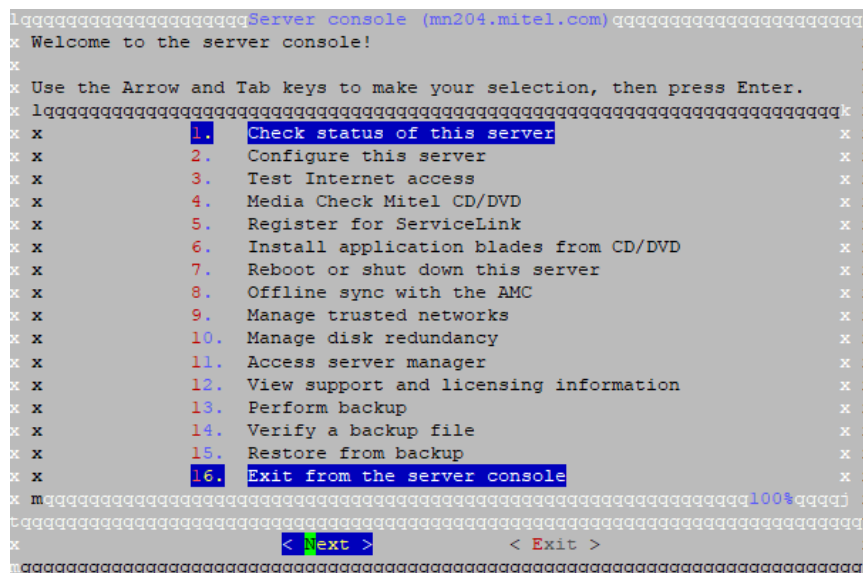


Figure 4: Server Console

5.5.2 Configure this Server

To configure this server:

1. In the Server Console main menu, click **2. Configure this server**, and then click **Next**.
2. In the configuration screens, enter the settings listed in the following table:

Screen	Action
Primary domain name	Enter the domain name (for example, mitel.com).
Enter system name	Enter a system name (for example, your company name)
Select local network adapters	Select one or more network adapters. i Note:

Screen	Action
	This screen is displayed only for an EX controller.

Screen	Action
	If you have restored a database from the MiVoice Business Virtual system in an EX controller, then after the restore, select eth1 virtio_net - <IP address of the adapter> [eth1: UP].
Local networking parameters	Enter an available IP address (without leading zeros) that is used to access both the Server Manager and the MiVoice Business system.
Enter local subnet mask	Enter the IP address of the subnet mask.
Enable IPv6 protocol	Specify whether you want to configure IPv6 addresses.
Static IPv6 address	Enter an available IP address that is used to access both the Server Manager and the MiVoice Business system.
Default IPv6 gateway	Enter the static IPv6 IP address gateway.
Select WAN network adapters	Select a network adapter. Skip if you have only LAN interfaces.
Enter gateway IP address	Enter the gateway IP address.
Corporate DNS server addresses	Enter one or more corporate DNS server IPv4 addresses, separated by a comma.
Resolve primary domain	Specify how MSL's DNS should resolve names for the domain.

3. Do one of the following:

- If you have modified only **DNS server addresses** configuration setting, click **Finish** to save the configuration changes.

The configuration settings are applied without rebooting the system.

- If you have modified any other configuration setting, click **Reboot**.

The configuration settings are applied upon system reboot.

5.5.3 Manage trusted networks

To manage trusted networks:

1. In the Server Console main menu, click **9. Manage trusted networks**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Trusted Networks Operations	• Click 1. Show trusted networks, and then click Next. The system displays the trusted IPv4 networks. • To add IPv4 trusted networks: a. Click 2. Add IPv4 trusted network, and then click Next. b. Enter the IP address, and then click Next. c. Enter the subnet mask, and then click Next. d. Enter the gateway IP address, and then click Next. • To delete the trusted IPv4 networks added: a. Click 3.Delete IPv4 trusted network, and then click Next. b. Click to select the network you want to delete, and then click Next. • To add IPv6 trusted networks: a. Click 4. Add IPv6 trusted network, and then click Next. b. Enter the IPv6 Trusted Network Address in the format Network/prefix (for example, 2016:a:b::/48), and then click Next. c. Enter the IPv6 Router Address, and then click Next. • To delete the trusted IPv6 networks added: a. Click 5.Delete IPv6 trusted network, and then click Next. b. Click to select the network you want to delete, and then click Next.

5.5.4 Perform backup

To back up the database:

- Samba (SMB)/Common Internet File System (CIFS)
- Secure File Transfer Protocol (SFTP) To back up the database:

i Note:

It is recommended to perform backup using Server Manager (**Administration > Backup**).

1. In the Server Console main menu, click **6. Perform backup**, and then click **Next**.
2. In the configuration screens, select the following settings:

Screen	Action
Backup server IP address	Enter the IP address of the network file share server where you want to store the database backup file.
Backup server domain or workgroup name	Enter the Domain or workgroup name. Applies only to SMB/CIFS. Leave the field blank for SFTP. Sets the SMB domain of the user name. If the domain specified is the same as the server's NetBIOS name, then the server's local Security Account Manager (SAM) is used for authentication, instead of the domain SAM. This field is required only for the SMB/CIFS protocol.
Backup share name	Enter the file-share name. Applies only to SMB/CIFS. Leave the field blank for SFTP. The restore utility will try to connect to the server/ shared folder as an SMB/CIFS resource. The shared folder must have permissions set to Full Control .
Optional Directory Path	Enter the name of the sub-folder where you have stored the database backup file. For SMB/CIFS, the sub-directory is relative to the share. For SFTP, the sub-directory is relative to the root of the file system accessed through the SFTP protocol.
Backup username	Enter the user name to use when connecting to the network file share server.
Backup password	Enter the password to use when connecting to the network file share server.
Proceed with Backup to network	Click Proceed .

The system creates a database backup file in the specified directory on the file server.

5.5.5 Verifying a Backup File

To verify previous backup files:

1. In the Server Console main menu, click **14. Verify a backup file**, and then click **Next**.
2. At the prompt, insert your storage medium. (Note: if your USB device was left mounted after your last backup, you must remove it and re-mount it first.)
3. If more than one storage device is connected to your system, select the device that contains the backup file.
4. If more than one backup file is contained on the storage device, select the file you want to verify.
5. Click **OK**. Verification of the file is confirmed. If you receive an error message, you cannot use this backup file for the restore. Check your storage media and try the backup procedure again.

Troubleshooting

6

This chapter contains the following sections:

- [System Software](#)
- [Reset/Default Button](#)
- [Reset the System Administration Tool Password](#)

This chapter provides troubleshooting information for the EX Controller, intended for use by Mitel certified technicians.

For troubleshooting other general issues, see *MiVoice Business Troubleshooting Guide*.

6.1 System Software

The following logs provide information for troubleshooting EX Controller issues:

- Software logs from the System Administration Tool (**Maintenance and Diagnostics > Logs > All Maintenance and Software Logs**)
- Log files from the Server Manager (**Administration > View Log Files**)
- EX Controller local logs from the EX Controller Web GUI (**System > Local Log**)

Note:

In the event of a system failure that requires assistance, collect log files and diagnostic data (SOS report) from the Server Manager before contacting Product Support.

Table 5: System Software Troubleshooting

Symptom	Possible Cause	Corrective Action
- Telephony cards are not listed in the Hardware Modules form in the MiVoice Business System Administration Tool. - Unable to perform backup from Server Manager. - Telephony cards are not functioning properly.	Unable to log into the EX Controller Web GUI as <i>mimx</i> user after a password reset using Server Manager	- Reset the <i>admin</i> user password from Server Manager to the same password. For example, if the old password is Company@123, reset the new password to Company@123. The system takes about 30 seconds to update the passwords of the user accounts on EX Controller. - If you are still unable to log into the EX Controller Web GUI as <i>mimx</i> user, then log into the EX Controller Web GUI as <i>public</i> user and navigate to Management > Access Control, and enter the Server Manager <i>admin</i> user password for the <i>mimx</i> user. - Repeat step 1 and monitor <i>/var/log/ex/ex.log</i> for <i>mimx</i> communication errors. If so, this could be due to network setup issues. Resolve the network setup issues.
	Incorrect configuration	- Check whether the System Administration Tool is up and running and is accessible. - Investigate whether the IP address of the EX Controller Web GUI has been modified. - Check for network issues. If the above corrective actions does not resolve the issue, perform a partial reset. See Partial Reset on page 78. If partial reset does not resolve the issue, perform a factory reset. See Factory Reset on page 81.

Symptom	Possible Cause	Corrective Action
Unable to access System Administration Tool.	The MiVoice Business software deployed on the EX Controller is corrupted.	• Check whether the MiVoice Business virtual machine deployed on the EX Controller is up and running. • Check whether you can access Server Manager. • Check whether you can generate the SOS logs from Server Manager (Administration > View log files) and collect SOS logs. • Check whether there is CPU hogging. • Check for network issues. • Access the MiVoice Business virtual machine through VNC Viewer and monitor the shell activity for issues. If you need help with any of the above corrective actions, contact Mitel Technical Support with SOS logs.
The EX Controller Deployment Tool virtual machine cannot be located on the EX Controller Web GUI.	The EX Controller Deployment Tool virtual machine is deleted from the EX Controller Web GUI.	Contact Mitel Technical Support.

Symptom	Possible Cause	Corrective Action
Cannot log into the System Administration Tool.	Forgot the login credentials	See Reset the System Administration Tool Password on page 85.
	- IP addresses (static IP address or the IP address provided by DHCP service) modified by someone - The network is misconfigured or is in an invalid state	- Check whether you can access the EX Controller Web GUI. - If the EX Controller Web GUI is accessible, then log in to the EX Controller using the VNC application by entering <IP address of the EX Controller Web GUI>:1, in the VNC Server field. Run the ifconfig command and verify whether eth1 has the correct MiVoice Business IP address. If not, modify the IP address of the MiVoice Business. To modify the MiVoice Business IP address, see Configure this Server on page 65.  Note: To enable VNC, see the Enabling the VNC Capability section. Collect SOS logs from Server Manager (Administration > View log files). If you need help with any of the above corrective actions, contact Mitel Technical Support with SOS logs.
Unable to log in to the EX Controller Web GUI	User account locked after multiple failed log in attempts	Check the syslog file generated from the EX Controller Web GUI to confirm whether the user account it locked. The account is automatically unlocked after a certain configurable duration (default is 300 seconds).  Note: Lock protection locks the user account after multiple (default is 5) failed log in attempts. Lock protection is enabled by default for a user. You can disable lock protection from Management > Access Control in the EX Controller Web GUI. Also, see the corrective actions described for Unable to log into the EX Controller Web GUI as mimx user after a password reset using Server Manager.

Symptom	Possible Cause	Corrective Action
- A Backup from the Server Manager (Administration > Backup) fails - MiVoice Business software logs indicate an issue with mimx or the EX system	Mismatch in: Passwords between MiVoice Business and the EX ControllerThe EX host address, and the address stored by MiVoice Business.	The ex-audit script detects: - a mismatch in mxTarget (EX Controller) ip address and ip0 property (MiVB) ip address - failure to initialize mimx (mivbMimxKeystoreInit) - improper file permissions for mimx folder - whether mimx has the proper settings to access the MiVB - whether mimx has the proper settings to access the EX Controller - whether the EX firmware matches the recommended version in the EX Blade software

Symptom	Possible Cause	Corrective Action
		Run the ex-audit script to check for any potential installation issues: 1. Log in to the system through SSH (for example, through PuTTY) as the <i>root</i> user. 2. Run the following command: <pre>/usr/ex/bin/ex-audit m5_ip_addr</pre> i Note: When executing the command, replace <i>m5_ip_addr</i> with the actual IP address of the EX Controller. Any issues are displayed with an "INFO:" text; usually, the command suggests using the '-a' option to repair the error. The '-f' option is suggested for a special case (see Step 4). 3. If the "INFO:" text suggests the '-a' option, run the following command: <pre>/usr/ex/bin/ex-audit -a m5_ip_addr</pre> 4. If the audit detects that both <i>mxTarget</i> and the <i>mimx</i> have not been initialized, run the command with the '-af' option: <pre>/usr/ex/bin/ex-audit -af m5_ip_addr</pre> 5. After running the '-a' or '-af' options, try the ex-audit script again to check for issues. If the following text is present: "Failed to communicate with <i>mxTarget</i>", there may be a password mismatch. Access the EX Controller and ensure that SNMP v2 is enabled. Then, use the ex-audit command with the '-r' option: <pre>/usr/ex/bin/ex-audit -r m5_ip_addr</pre>
		This resets the passwords to default1 on both the <i>mimx</i> and EX Controller. Access the Server Manager and reset the admin password to align the credentials for some applications. If SNMP v2 was previously disabled, access the EX Controller and disable it.

6.2 Reset/Default Button

The **Reset/Default** button can be used to perform a factory or partial reset of the EX controller while the unit is powered on.

The **Reset/Default** button will generate different actions depending on the duration of time the button is held.

Pressing Time	Action	Comment	LED Pattern
2 to 6 seconds	Restarts the EX Controller.	No changes are made to the EX Controller settings.	Power1 blinking, all other LEDs Off.
7 to 11 seconds	Initiates a Partial Reset of the EX Controller	Restarts the unit in a known and static state while keeping most of the configuration unchanged.	All LEDs blinking, 1cycle per second, 50% duty.
12 to 16 seconds	Initiates a Factory Reset of the EX Controller	Reverts the unit to its default factory settings. For more information, see Factory Reset on page 81.	All LEDs steady On.
17 seconds and more	No action is taken. This is useful if you accidentally pushed the button and do not need an action to be applied.	The action is ignored.	All LEDs will become Off after blinking and being steady on.

6.2.1 Partial Reset

You can perform a partial reset of the EX Controller to:

- Reset the password of the EX Controller Web GUI. For example, if you have forgotten the password.
- Contact the unit in a known state when you can no longer access the EX Controller Web GUI. For example, due to modified configuration. In such case, you can manage the EX Controller using the

Rescue Network Interface. The Rescue Network Interface is bound to the WAN port ETH1 of the unit and accessible through the IP address 192.168.0.1. (IPv4) or an IPv6 Link Local address.

The Rescue Network Interface is used for:

- Completing the configuration of a new unit.
- Modifying existing configuration.

By default, the Rescue Network Interface is disabled. When a partial reset is performed, the Rescue Network Interface becomes enabled and the **Power** and **Ready** LEDs are blinking at 1Hz with 75% duty and all other LEDs are off. Once the configuration has been modified to solve the problem that required the partial reset, it is important to disable the Rescue Network Interface to make sure that you are no longer working in the Rescue Network Interface.

Partial reset on a new EX Controller does not modify its configuration. However, a partial reset performed on an EX Controller already in use will:

- Rollback Local Firewall settings that are not yet applied.
- Add a Local Firewall rule to allow complete access to the Rescue Network Interface.
- Rollback NAT settings that are not yet applied.
- Cancel the changes that were being modified but not yet applied to the configuration.
- Add NAT rule to allow complete access to the Rescue interface.
- Disable any Network Interface in conflict with the Network Rescue Interface.
- Configure and enable the Rescue Network Interface to:
 - use the link as the default value used by Uplink Network interface
 - set the IP address to 192.168.0.1 and the Network Mask to 255.255.255.0
 - set the IPv6 link-local address on all network links. The IPv6 link-local address can be underneath the EX Controller.

A partial reset will also modify the following parameters and preserve the values below even after the Rescue Network Interface has been disabled.

Service	Parameter	Default Value
AAA	Users.Password	<i>admin</i> and <i>pubic</i> users from profile are restored with their factory password. All other user names keep their password.
	Users.AccessRights	User(s) from profile are restored with their factory rights.
	ServicesAaaType (table)	Each service will be configured to use Local authentication and no accounting mechanism.
CLI	EnableTelnet	Disable

Service	Parameter	Default Value
	TelnetPort	23
	EnableSsh	Enable
	SshPort	22
	InactivityTimeOut	15
HOC	ManagementInterface	Rescue
SNMP	Port	161
	EnableSnmpV1	Enable
	EnableSnmpV2	Enable
	EnableSnmpV3	Enable
Web	ServerPort	80
	SecureServerPort	443

To perform a partial reset of an EX Controller:

1. On a controller that is powered on, insert a small unbent paper clip into the hole of the **Reset/Default** button located at the front of the unit.
2. Press and hold the **Reset/Default** button for 7 to 12 seconds until all LEDs are blinking.
3. When all the LEDs are blinking, remove the paper clip.

Note:

The Power LED starts blinking.

4. After you perform the partial reset, the **public** password is set to the factory default as blank. The EX Controller Web GUI is accessible using ETH1 and the IP address 192.168.0.1.

5. Set the Server Manager *admin* user password as the password for the *mimx* user and resolve any networking issue before disabling the Rescue Network Interface. To do so:
 - a. Log in as **public** to the EX Controller Web GUI.
 - b. Click **Management > Access Control**.
 - c. Set the *mimx* password to the same one used as the Server Manager *admin* user password.
 - d. Click **Apply**.
 - e. Click **Management > SNMP**.
 - f. Set the SNMP V3 password to the same one used as the Server Manager *admin* user password.
 - g. Click **Apply**.

i Note: See the corrective action described for [Telephony cards are not listed in the Hardware Modules form in the MiVoice Business System Administration Tool](#) on how to set the Server Manager *admin* user password as the password for the *mimx* user.

6. Disable the Rescue Network Interface:
 - a. [Log in to the EX Controller Web GUI](#) on page 47.
 - b. Click **Management > Misc**.
 - c. From the **Network Interface** drop-down menu, select **All** as the interface that will be used to manage the EX controller unit.

i Note: If the Rescue Network interface is enabled, the **Management** interface will be inaccessible after you disable the Rescue Network interface.

- d. Click **Apply**.
- e. Click **Network > Interfaces**.
- f. From **Rescue Network Configuration**, in the **Activation** list, select **Disable**.
- g. Click **Apply**.

The EX Controller unit will be inaccessible on the newly configured static IP address or on the DHCP server.

7. Log in to the Server Manager and reset the password to synchronize the user account passwords with the Server Manager password.
8. Enable SNMP v1, v2, and v3 from Server Manager (**Configuration > SNMP**).

6.2.2 Factory Reset

Depending on the DGW firmware version running on the EX Controller, the factory reset defaults the controller's IP scheme and deletes the persistent configuration parameters of the unit, including:

- MiVoice Business virtual machine and its database¹
- MiVB.img and MiVB.cfg files¹
- User files stored in the File service
- Certificates, except for the factory installed ones
- Log files of the File service

¹A factory reset on EX Controllers running DGW firmware lower than 45.1.1870 does not fully restore to its default settings, that is, the MiVoice Business virtual machine, database, MiVB.img and MiVB.cfg files are left undeleted in the controller. However, with EX Controllers running DGW firmware 45.1.1870, a factory reset restores the controller to its default settings. Therefore, it is recommended to upgrade to the DGW firmware 45.1.1870 by upgrading the MiVoice Business EX software to the version 9.0.3.15_2 using Server Manager.

Factory reset must be performed on an EX Controller unit that is isolated from the network with access to a DHCP server. If the unit cannot find a DHCP server, it sends requests indefinitely.

Note:

Restoring factory default settings erases the deployment parameters.

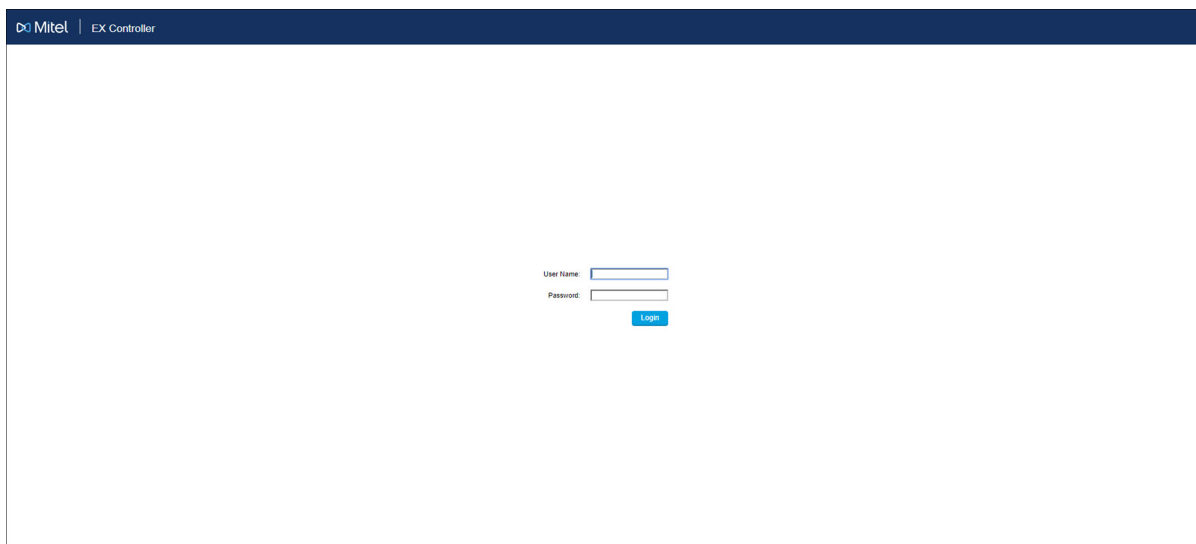
To perform a factory reset of the EX Controller running DGW firmware version 45.1.1870 or higher:

1. On a controller that is powered on, insert a small unbent paper clip into the hole of the **Reset/Default** button located at the front of the unit.
2. Press and hold the **Reset/Default** button for 12 to 16 seconds until all the LEDs are steadily on. The controller unit reboots with the default IP address 192.168.0.10 accessible through **ETH2-ETH5** of the EX Controller.
3. Continue with [Accessing the EX Controller Deployment Tool](#) on page 31.

To perform a factory reset of the EX Controller running DGW firmware version lower than 45.1.1870:

1. On a controller that is powered on, insert a small unbent paper clip into the hole of the **Reset/Default** button located at the front of the unit.
2. Press and hold the **Reset/Default** button for 12 to 16 seconds until all the LEDs are steadily on. The controller unit reboots with the default IP address 192.168.0.10 accessible through **ETH2-ETH5** of the EX Controller.
3. Assign a static IP address to your PC using the following IP scheme:
 - IP address: 192.168.0.100
 - Subnet mask: 255.255.255.0
 - Gateway IP address: 192.168.0.1
4. Connect an RJ45 Ethernet cable from the PC's Ethernet interface to any one of the ports **ETH2 - ETH5** of the EX Controller.

- Enter the IP address 192.168.0.10 in the address bar of your browser to access the EX Controller Web GUI.



Mitel | EX Controller

User Name:

Password:

Login

The EX Controller Web GUI login page is displayed.

- In the **User Name** field, type **public**.
- Leave the **Password** field empty.
- Click **Login**.

The EX Controller Web GUI home page is displayed.



Mitel | EX Controller

System Network SBC Management Reboot

Information Services Hardware Event Log Local Log Packet Capture Diagnostic VM

• Information

Current Status	
Device Identification:	EX Controller
Firmware:	Dgw 44.3.1746
Profile:	STNL-MT-D2000-155
MAC Address:	0090f80bdc8
Serial Number:	000400001M318170017
Number of DSPs:	0
Storage Memory (in use/total):	18.3 GB / 60 GB
Volatile Memory (in use/total):	2.3 GB / 8 GB
System Uptime (D:HH:MM:SS):	12:19:04:19
System Time (DD/MM/YYYY HH:MM:SS):	28/11/2019 02:34:15

Licences	
CWMP/TR-069	
SBC Licence for 3 concurrent sessions	
Virtual Machine Licence	

Activate Licence	
Licence Key:	

Apply

9. Delete **MiVB.img** and **MiVB.raw** files:

- a. Click **Management > File**. The **File** page is displayed.
- b. From the **VM Files** table, click  to delete **vm/images/MiVB.cfg** and **vm/images/MiVB.raw** files.

Note:

Do not delete **vm/images/exdeploy.cfg** and **vm/images/exdeploy.img** files.

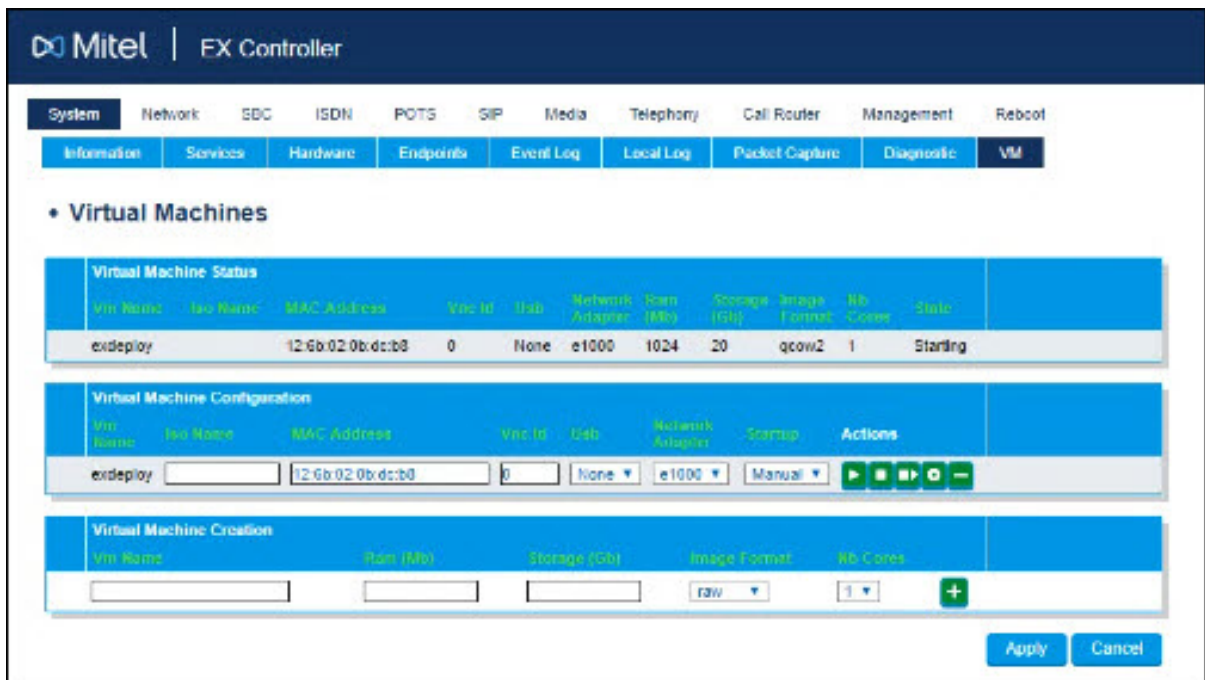
VM files			
Name	Description	Size	
vm/images/exdeploy.cfg	Virtual Machine configuration file	1 KB	
vm/images/exdeploy.img	Virtual Machine image file	8.7 GB	
vm/images/MiVB.cfg	Virtual Machine configuration file	1 KB	
vm/images/MiVB.raw	Virtual Machine image file	31.3 GB	
4 file(s)		Total: 40 GB / Available: 5.6 GB	

A confirmation message is displayed.

- c. Click **OK** to delete the files.

10. Start the Deployment Tool virtual machine:

- a. Click **System > VM**. The **Virtual Machine** page is displayed.
- b. Under **Virtual Machine Configuration** section, change **Startup** option to **Auto** for the **exdeploy** virtual machine configuration.



- c. Click  to start the Deployment Tool virtual machine. After a minute, refresh the page. The **State** under the **Virtual Machine Status** changes to **Starting** from **Stopped**. After a minute, the **Virtual Machine Status** changes to **Started**.
- d. Continue with
 - i. [Accessing the EX Controller Deployment Tool](#) on page 31.
 - ii. [Updating the EX Controller Deployment Tool](#) on page 32.
 - iii. [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#) on page 34.

6.3 Reset the System Administration Tool Password

Overview

If you are unable to log in to the System Administration Tool as the *system* user, then you can reset the password for *system*.

Procedure

1. Log in to the system through SSH (for example, through PuTTY) as the *root* user.

2. Run the following command to reset the *system* password:

mcdDebug ResetLoginPassword system

3. Press CTRL + C to exit the mcdDebug shell.

4. Run the **logout** command to log out of the system:

Appendix A: Assigning a Static IP Address to the EX Controller Deployment Tool

7

This chapter contains the following sections:

- [Assigning a static IP address manually](#)
- [Assigning a static IP address by using a USB flash drive](#)

If a DHCP server is not available on the network on which you want to deploy the EX Controller or if you are unable to access the Deployment Tool using a DHCP server, then you can access the Deployment Tool by assigning a static IP address to the Deployment Tool either [manually](#) or [using a USB flash drive](#).

7.1 Assigning a static IP address manually

Prerequisites

- An RJ45 Ethernet cable for connection between the EX Controller and Layer2 switch.
- Download and install the latest version of UltraVNC Viewer (or VNC Viewer) application installed on the deployment PC.

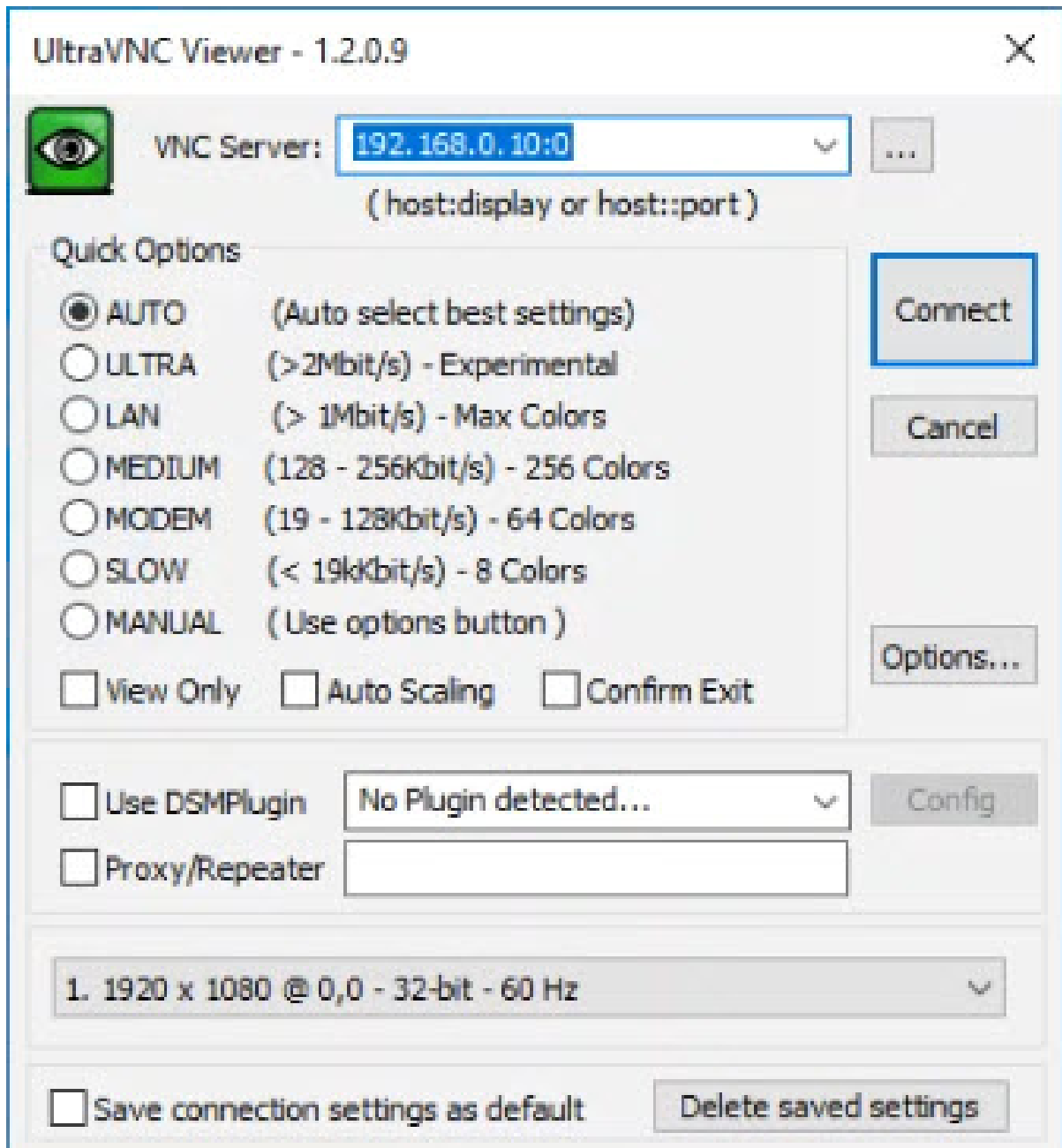
 **Note:** To enable VNC, see the [Enabling the VNC Capability](#) section.

Procedure

To manually assign a static IP address to the Deployment Tool:

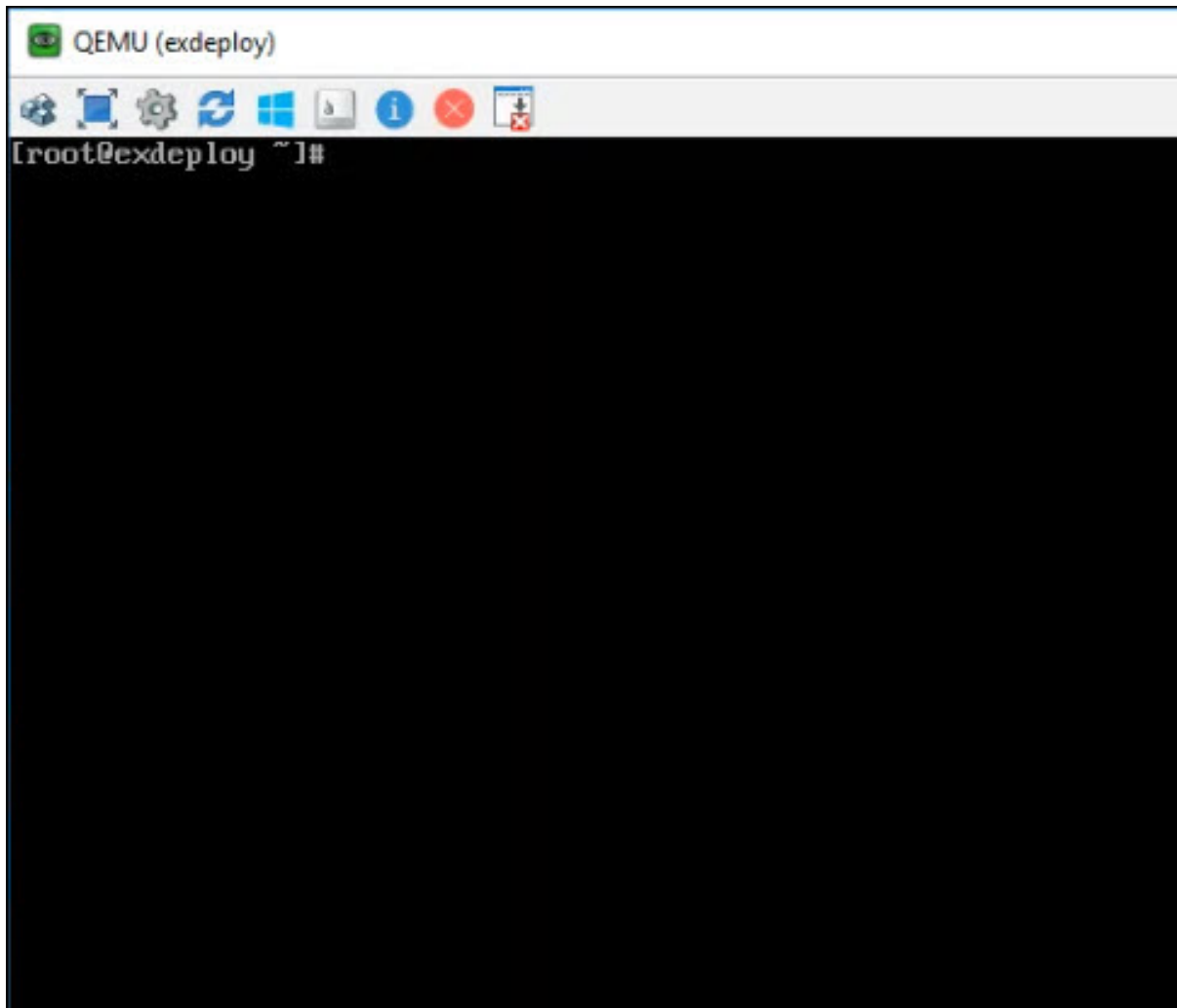
1. Assign a static IP address to your deployment PC using the following IP scheme:
 - IP address: 192.168.0.100
 - Subnet mask: 255.255.255.0
 - Gateway IP address: 192.168.0.1
2. Power on the EX Controller.
3. Connect an RJ45 Ethernet cable from the deployment PC's Ethernet interface to one of the **ETH2 - ETH5** ports of the EX Controller.
4. From the deployment PC, start **UltraVNC Viewer**.

5. In the **VNC Server** field, enter < **Default IP address of the EX Controller Web GUI** > :0. The default IP address of the EX Controller Web GUI is **192.168.0.10**.



6. Click **Connect**.

The Deployment Tool virtual machine console is displayed.



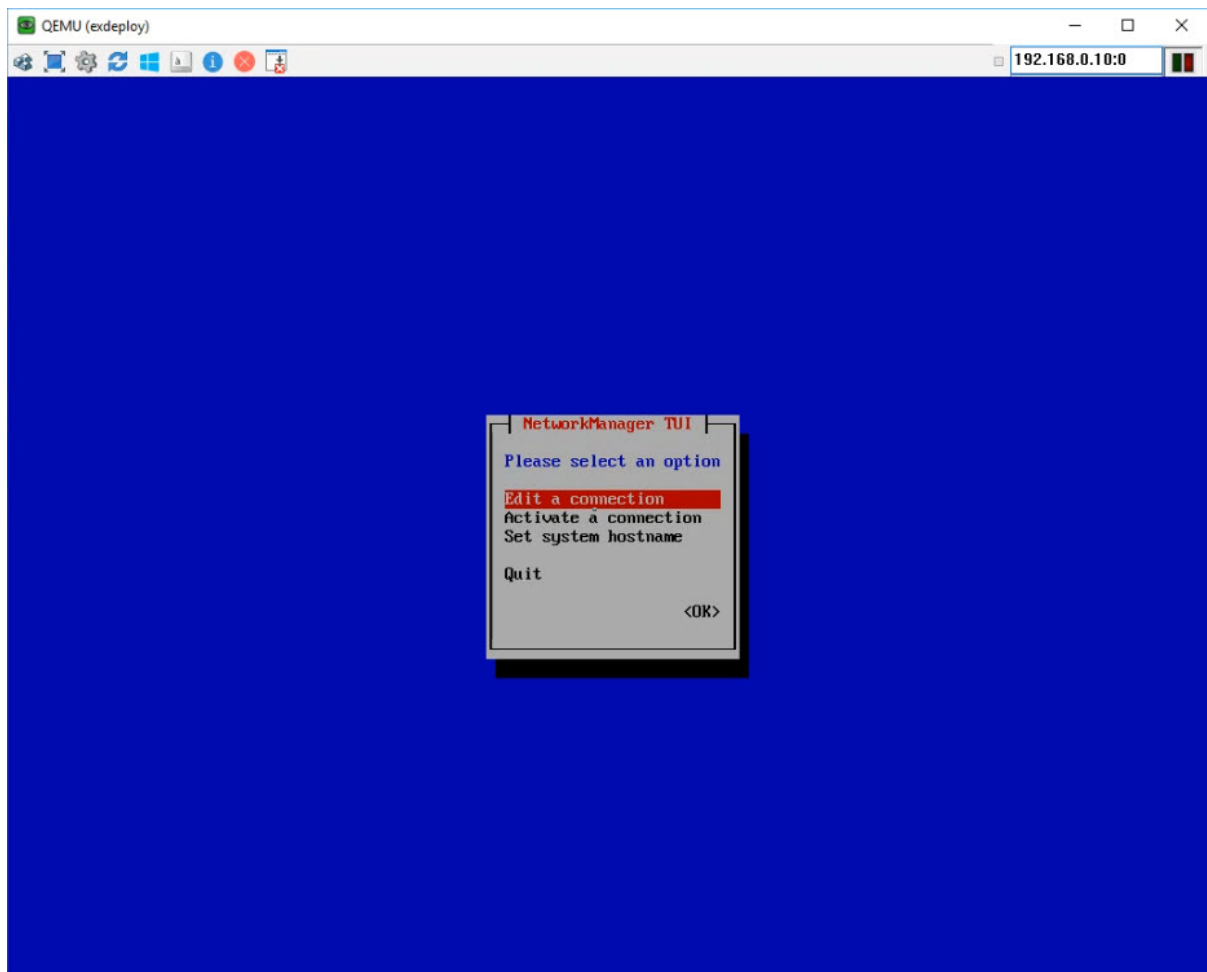
7. Log in as *root* user. The default password for *root* user is **default**.

8. Execute the following command to set **ens4** to a static setting:

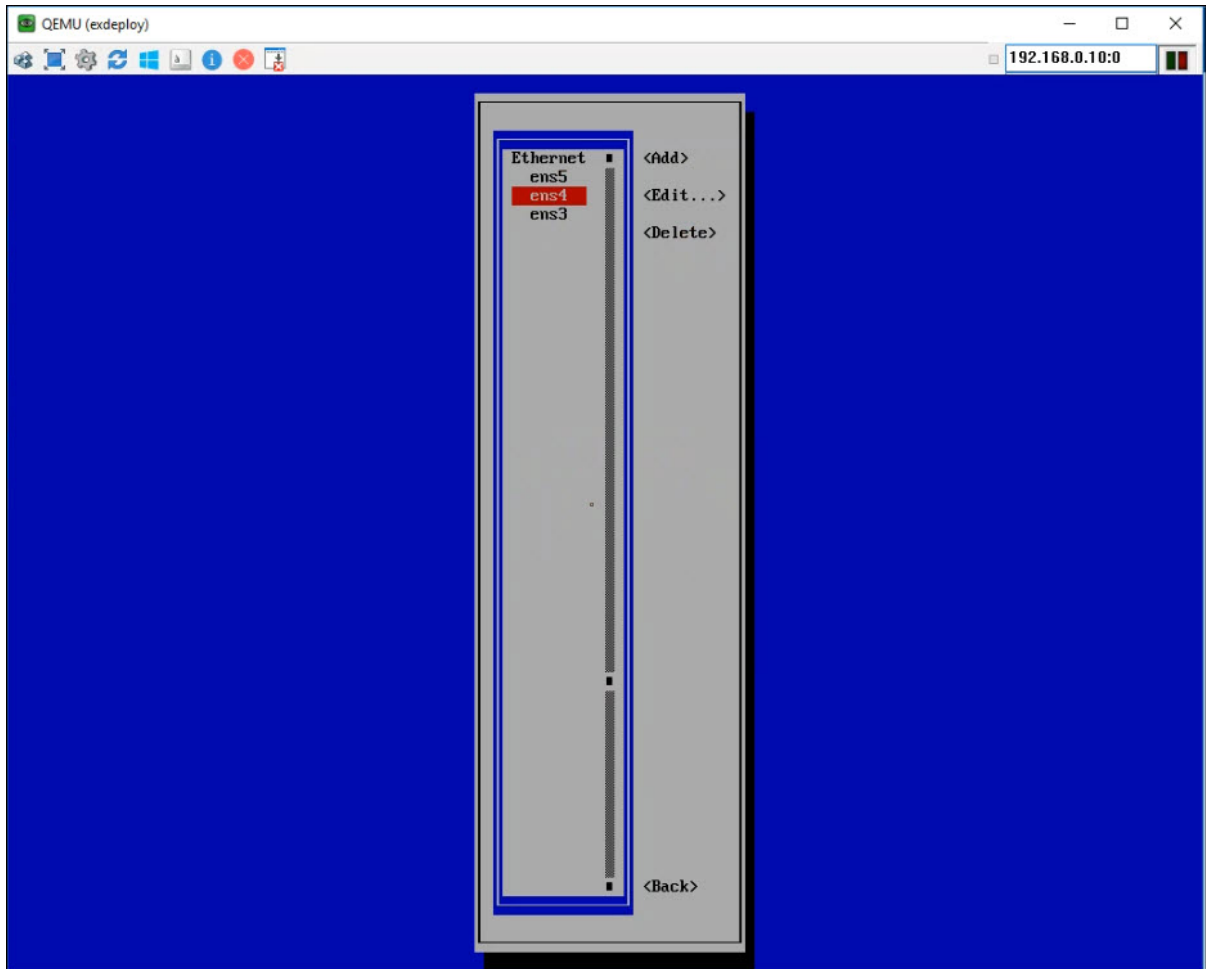
```
nmtui
```

The Network manager TUI screen is displayed.

9. From the options, select **Edit a connection** and press Enter.



- From **Ethernet**, select **ens4** and select **Edit** to edit the LAN interface of the Deployment Tool virtual machine.



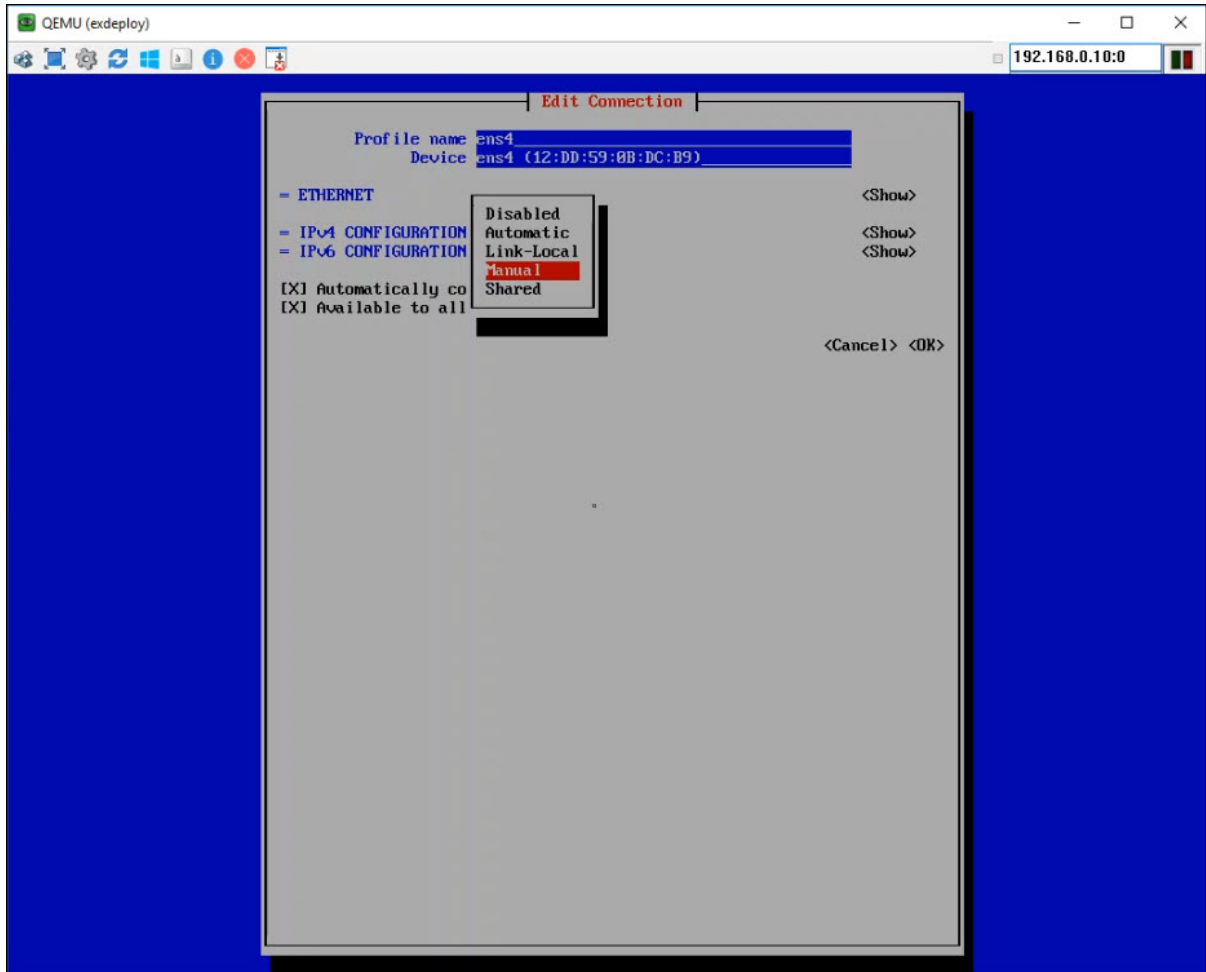
Note: The **ens3** option is used to edit the WAN interface, and the **ens5** option is used edit the private interface that communicates with the EX Controller. Do **NOT** modify these options.

- Press Enter.

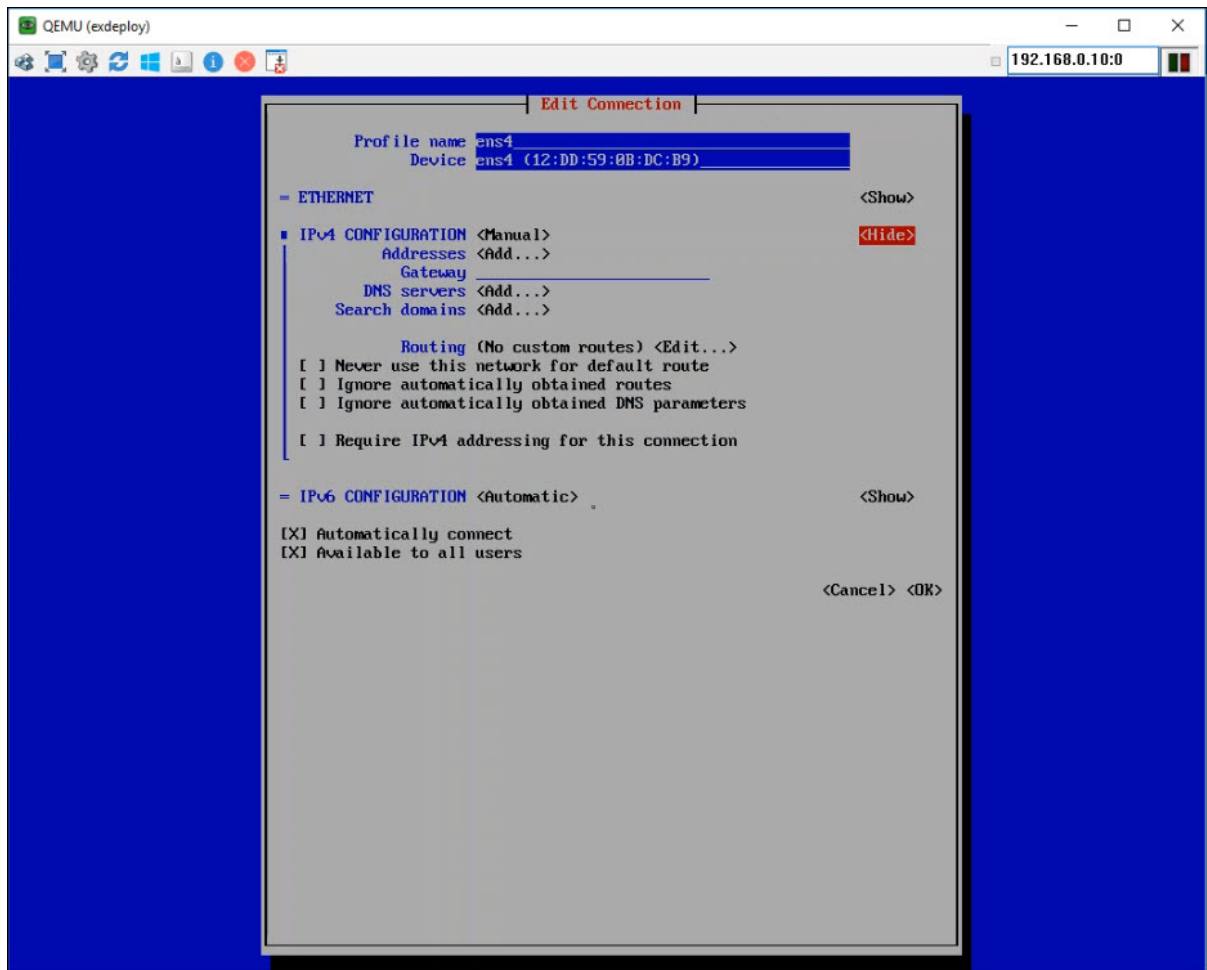
The **Edit Connection** screen is displayed.

- Navigate to **IPv4 CONFIGURATION <Automatic>**, and press Enter.

13. From the dialog box, select **Manual**.



14. Select **<Show>** next to **IPv4 CONFIGURATION**, press Enter to expand the IP address configuration section.



15. Enter the following:

- a. **Addresses**—An available static IP address in the LAN for the Deployment Tool virtual machine.

Note:

You can also enter a private IP address, such as 192.168.x.x, which can be accessed by the deployment PC only through 192.168.x.x interface.

- b. **Gateway**—Gateway IP address of the LAN.

16. Select **OK** and press Enter.

The Network Manager TUI screen is displayed.

17. Click **Back** to save the configuration.

18. Click **Quit** to exit the Network Manager TUI screen.

The Deployment Tool virtual machine console is displayed.

19. Restart the network stack by executing the following command at the prompt for the changes to take effect:

```
systemctl restart network
```

20. Verify that the Deployment Tool virtual machine has the specified static IP address. Run the **ifconfig** command and verify whether the correct IP is assigned to **ens4**.

```

[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]#
[root@exdeploy ~]# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    ether 12:c4:95:0b:dc:be txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 417 bytes 79548 (77.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.37.27.85 netmask 255.255.255.0 broadcast 10.37.27.255
    inet6 fe80::616c:ca14:f6fd:dbd prefixlen 64 scopeid 0x20<link>
    ether 12:c4:95:0b:dc:bf txqueuelen 1000 (Ethernet)
    RX packets 2566 bytes 157204 (153.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 375 bytes 64160 (62.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 169.254.10.2 netmask 255.255.255.0 broadcast 169.254.10.255
    inet6 fe80::416d:509e:004b:f1f7 prefixlen 64 scopeid 0x20<link>
    ether 12:c4:95:0b:dc:c0 txqueuelen 1000 (Ethernet)
    RX packets 4 bytes 718 (718.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 124 bytes 18703 (18.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@exdeploy ~]#
  
```

21. Do one of the following:

- If you have specified a static IP address from the LAN, then do the following:
 - a. Disconnect the Ethernet connection between your deployment PC and the controller.
 - b. Connect an RJ45 Ethernet cable from any one of the **ETH2** to **ETH5** ports of the EX Controller to the Layer2 switch on the LAN.
 - c. Revert your deployment PC's IP scheme to **Obtain an IP address automatically**.
 - d. Connect an RJ45 Ethernet cable from your deployment PC to the to the Layer2 switch on the same LAN.
- If you have specified a private network address (192.168.x.x), leave the EX Controller connected to the deployment PC.

22. Open a web browser (recommended Mozilla Firefox and Google Chrome), and type the IP address (specified in **step 15 (a)**) in the address bar, and press Enter.

The EX Controller Deployment Tool home page is displayed.

23. Continue with [Updating the EX Controller Deployment Tool](#) on page 32.

7.2 Assigning a static IP address by using a USB flash drive

Note:

For using the USB flash drive to assign a static IP address to the EX controller deployment tool, the installed EX deployment tool must be version 1.1.13.0 or higher. An upgrade of the EX deployment tool might be required for the process to function properly.

Objective

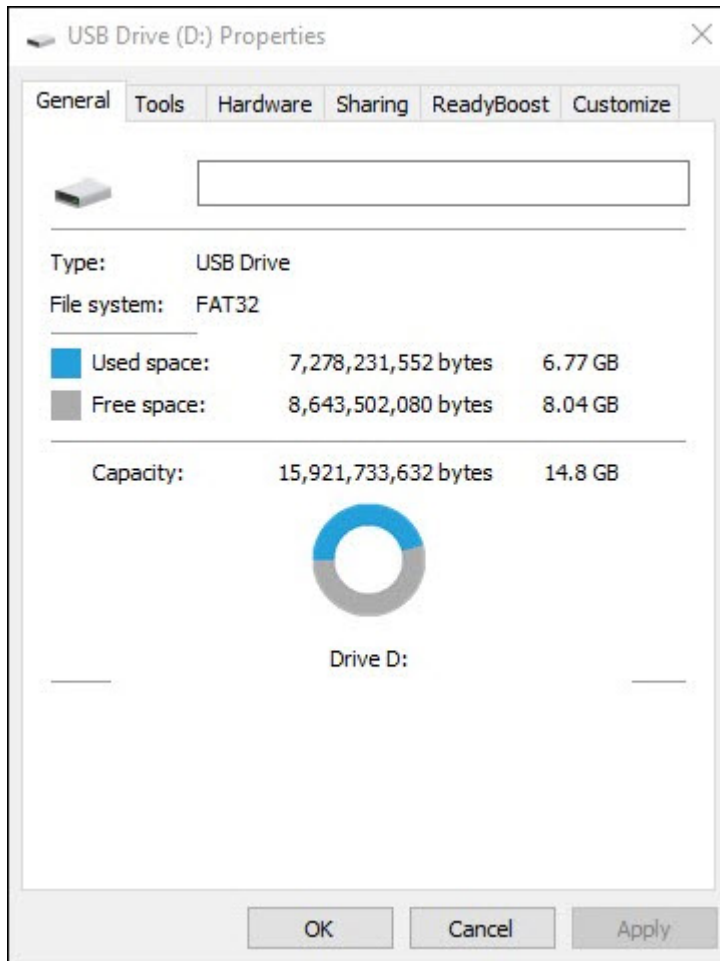
If an appropriately loaded USB flash drive is installed in the USB port on the front of the EX controller during boot, the EX deployment tool will use the IP address in the `lan.cfg` file located on the USB drive.

Prerequisites

- A USB flash drive with minimum 8-GB memory with FAT32 file system.

Note:

To verify the file system of the USB flash drive, insert the USB flash drive into your PC. Right-click the USB flash drive, and click **Properties**.



Procedure

1. Copy the downloaded files **exdeploy-x.x.x.x.zip** and **MiVB-x.x.x.x-yy.img.zip** from your deployment PC to the USB flash drive.

2. Create a **lan.cfg** file with the static IP address and gateway IP address in the following format and copy the file to the USB flash drive:

addr=<static IP address/CIDR>

gateway=<IP address>

For example:

addr=10.38.75.41/24

gateway=10.38.75.1

i Note: You can use a Notepad to create the lan.cfg file.

3. Connect the USB flash drive to either of the USB port of the EX Controller. See [Connection Interfaces and LEDs](#) on page 14.
4. Power on the EX controller or reboot it to allow the USB flash to be used.

i Note: Before proceeding to the next step, you must wait for approximately 5 minutes for the power on/reboot to complete.

5. The EX controller deployment tool can be accessed using the IP address provided in the lan.cfg file above.
6. Continue with either [upgrading the EX Controller Deployment tool](#) or proceed with the deployment.

Appendix B: Programming R2 Trunks

8

Overview of programming R2 Trunks

The R2 Trunk requires a standard **E1/T1 PRI** card to be installed in the EX Controller. To install these cards, the Mitel EX platform must be turned off. These cards are displayed as "**1PRI**" in the **MiVoice Business System Administration Tool**, in the **Hardware Modules** form.

Hardware Modules			
Slot Number	Module ID, Driver ID	Variant ID	Card Description
1			1 PRI
2			DSP
3			4 FXO
4			4 FXS
5			4 FXS LP
6			

Note:

- All programming must be done from the **MiVoice Business System Administration Tool**.
- When performing **Steps to program R2 Trunk on an EX Controller**, know that:
 - A new **Network element** entry will be automatically created with the name used in **Step 4** of the procedure **Steps to program R2 Trunk on an EX Controller**.
 - A new **SIP Peer Profile** will also be created with the name used in **Step 4** of the procedure **Steps to program R2 Trunk on an EX Controller**.
- Do not modify or delete these entries. They are used to route calls between MiVB and the R2 Trunks on the Mitel EX host platform.

Steps to program R2 Trunk on an EX Controller:

1. Ensure that any earlier programming for the card slot that will be used for R2 Trunk is removed.
 - **ARS Digits Dialed** and **ARS Routes** are cleared
 - **Gateway Trunks** is cleared for the appropriate cards

2. Program the **Gateway Trunk Descriptor**. Select the correct card and set the following:

- **Line Type = E1**
- **Signaling = R2**

Note:

- The above changes will prompt a system reboot. Choose **EX Platform Reboot** from the server manager.
- Rebooting the MiVB from the System Administration Tool does not reboot the host EX platform.

Change

Gateway Trunk Descriptors

Warning: Any changes to this record may be service affecting.

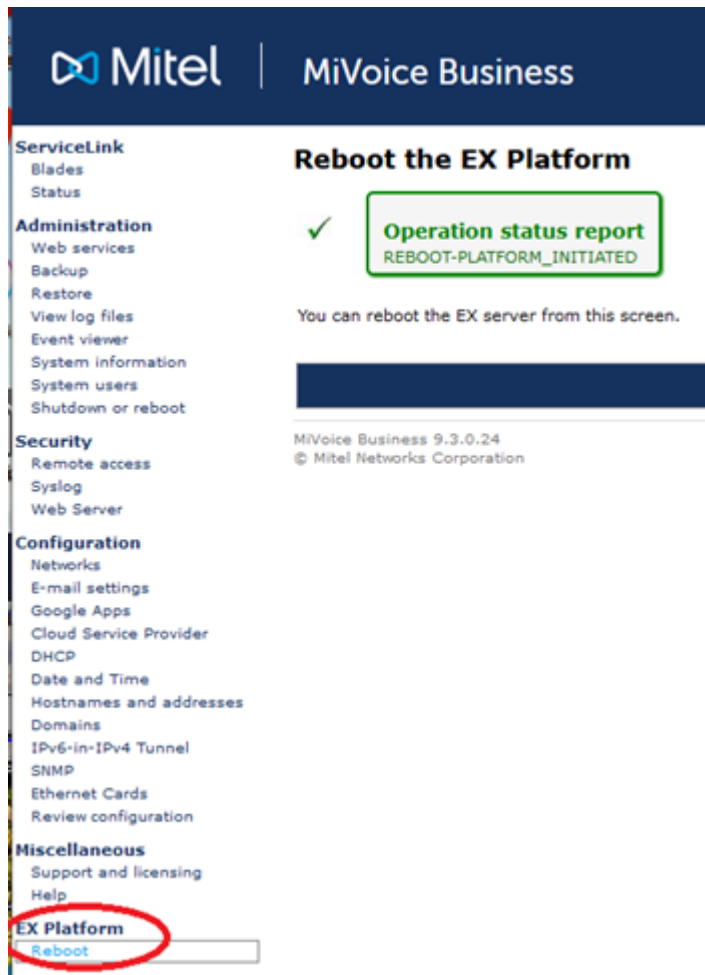
Gateway	10.37.27.80
Endpoint Id	Slot1/E1T1
Trunk Type	PRI
Link State	Down
Line Type	☐ T1 ☒ E1
Signaling	R2
Endpoint Type	☒ Te ☐ NT

Changing this value will only take affect after a system reboot.

Save Cancel

3. From the server manager, **Reboot** the **EX Platform**.

Note: The system reboot takes 5-10 minutes to complete.



4. Program the Gateway Trunk Profiles

- Provide a unique **Name**
- Add the required:
 - **Trunk Service Number**
 - **Class of Service (COS)**
 - **Class of Restriction (COR)**
 - **Dial In Trunks Incoming Digit Modification – Absorb**

Add

Gateway Trunk Profiles

Gateway	10.37.27.80
Name	EXR2trunk
Zone	1
Trunk Attributes	
Trunk Service Number	8
Class of Service	8
Class of Restriction	8
Non-dial In Trunks Answer Point - Day	
Non-dial In Trunks Answer Point - Night 1	
Non-dial In Trunks Answer Point - Night 2	
Dial In Trunks Incoming Digit Modification - Absorb	0
Dial In Trunks Incoming Digit Modification - Insert	
Incoming DID Range	
SIP Peer Profile	
Default CPN	

Save **Cancel**

5. Program the **Gateway Trunks** form

- Select the correct card slot
- Assign the new **Trunk Profile** in the **Gateway Trunk** form

Change

Gateway Trunks

Gateway	10.37.27.80
Endpoint Id	Slot1/E1T1
Trunk Profile	EXR2trunk

Save

Cancel

Gateway Trunks		
Gateway	Endpoint Id	Trunk Profile
10.37.27.80	Slot1/E1T1	EXR2trunk
10.37.27.80	Slot3/FXO1	
10.37.27.80	Slot3/FXO2	
10.37.27.80	Slot3/FXO3	
10.37.27.80	Slot3/FXO4	

6. Run the appropriate Gateway Configuration Script.

- In the **Gateway Configuration Scripts** form:
 - Select the correct card slot
 - Select the required **Default configuration files**
 - Select the **Execute** button and the select **OK**
- **Executing file** and then **Executing file...Success** will be displayed in the **Default configuration files** selection box

Note: Running the **Gateway Configuration Script** pushes the granular R2 programming into the Mitel EX host platform for the required R2 protocol.

Gateway Configuration Scripts

Enterprise Gateway Server: 10.37.27.80 v

Slot1/E1T1 v

Default configuration files: mitel_R2_Mexico_perislot.cfg v

Executing file... Success Export Execute

Export the current configuration for trunks of type: E1T1 v

Export

Import configuration from file: Browse... Import

7. Program the required **ARS Routes** and **ARS Digits Dialed** to use for the R2 Trunk. When programming the **ARS Routes**, select the following:

- **Route Medium** = SIP Trunk/Enterprise Gateway
- **SIP Peer Profile** = "Name given to the **Gateway Trunk Profiles**" from **Step 4** of the procedure **Steps to program R2 Trunk on an EX Controller**

Change

ARS Routes

Route Number	8
Routing Medium	SIP Trunk/Enterprise Gateway ▾
Trunk Group Number	
SIP Peer Profile	EXR2trunk ▾
PBX Number / Cluster Element ID	
COR Group Number	1
Digit Modification Number	1
Digits Before Outpulsing	▾
Route Type	▾
Compression	Off ▾

Save

Cancel

Appendix C: Enabling USB Ports for the Deployment Tool

9

The Deployment Tool version 1.1.13 supports installation of MiVoice Business software image and upgrade of the Deployment Tool using a USB flash drive. This requires the USB ports on the EX Controller to be enabled for the Deployment Tool. For EX Controllers that do not have the version 1.1.13 pre-installed, the USB ports are disabled for the Deployment Tool by default.

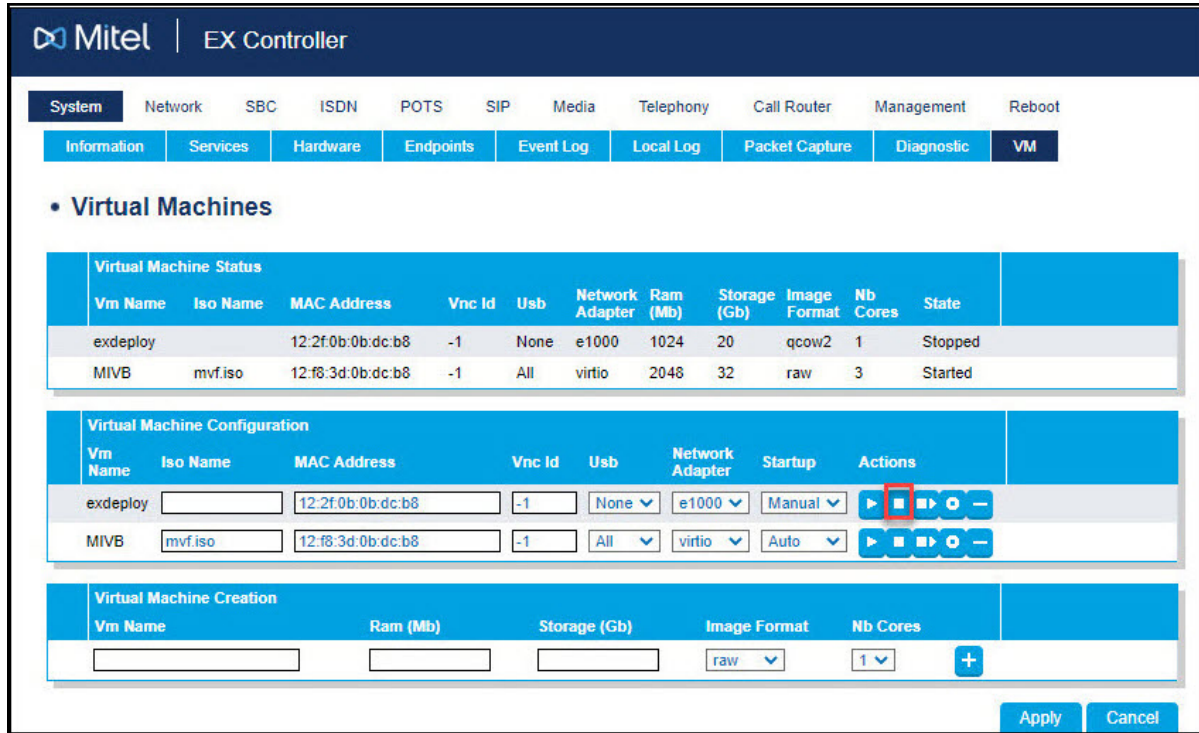
Procedure

Perform the following procedure to check and enable the USB port for the Deployment Tool, and to allow the Deployment Tool to use all three CPU cores:

1. [Upgrade the Deployment Tool](#) to version 1.1.13 or later.
2. [Log in to the EX Controller Web GUI](#) on page 47.
3. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

4. Click  under **Actions** to stop the **exdeploy** virtual machine.



Mitel | EX Controller

System Network SBC ISDN POTS SIP Media Telephony Call Router Management Reboot

Information Services Hardware Endpoints Event Log Local Log Packet Capture Diagnostic **VM**

• **Virtual Machines**

Virtual Machine Status										
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State
exdeploy		12:2f:0b:0b:dc:b8	-1	None	e1000	1024	20	qcow2	1	Stopped
MIVB	mvf.iso	12:f8:3d:0b:dc:b8	-1	All	virtio	2048	32	raw	3	Started

Virtual Machine Configuration									
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions		
exdeploy		12:2f:0b:0b:dc:b8	-1	None	e1000	Manual			
MIVB	mvf.iso	12:f8:3d:0b:dc:b8	-1	All	virtio	Auto			

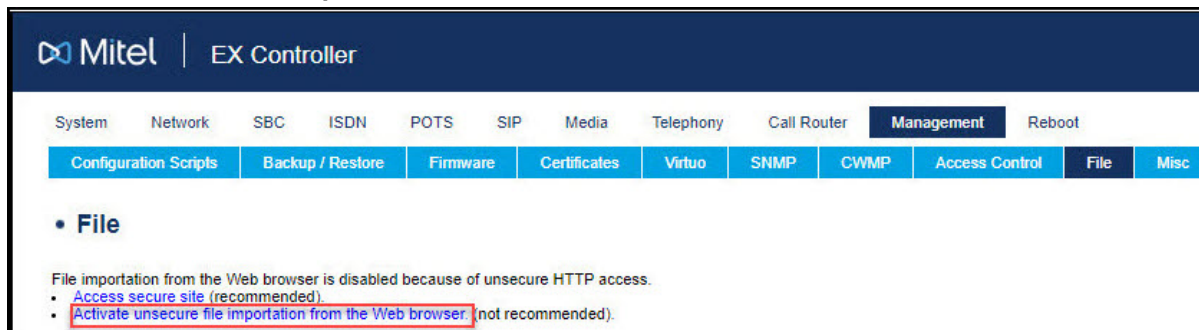
Virtual Machine Creation					
Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	
			raw	1	

Apply Cancel

Note: The VNC is disabled by default. To re-enable VNC for the **exdeploy** virtual machine or MiVoice Business virtual machine:

- Click  to stop the required virtual machine
- Enter a value (typically 0 for **exdeploy** virtual machine and 1 for MiVoice Business virtual machine) in the **Vnc Id** field.
- Click **Apply** to apply the changes.
- Click  to start the virtual machine.

- Change the **Usb** list corresponding to **MIVB** from **None** to **All**, and then click **Apply**. If **All** is already selected in the **Usb** list, skip this step.
- Click  corresponding to **exdeploy** to start the **exdeploy** virtual machine.
- Navigate to **Management > File**. If you are accessing the EX Controller using HTTP (not HTTPS), click **Activate unsecure file importation from the Web browser**.



Mitel | EX Controller

System Network SBC ISDN POTS SIP Media Telephony Call Router **Management** Reboot

Configuration Scripts Backup / Restore Firmware Certificates Virtuo SNMP CWMP Access Control **File** Misc

• **File**

File importation from the Web browser is disabled because of unsecure HTTP access.

- [Access secure site \(recommended\)](#).
- Activate unsecure file importation from the Web browser** (not recommended).

8. Scroll down to the **VM files** table, click **vm/images/exdeploy.cfg** to download the exdeploy.cfg file to your PC.

VM files		
Name	Description	Size
vm/images/factory/exdeploy.cfg	Factory Virtual Machine configuration file (read-only)	1 KB
vm/images/factory/exdeploy.img	Factory Virtual Machine image file (read-only)	2.6 GB
vm/images/exdeploy.cfg	Virtual Machine configuration file	1 KB
vm/images/exdeploy.snapshot	Virtual Machine snapshot image file	6.3 GB
vm/images/MIVB.cfg	Virtual Machine configuration file	1 KB
vm/images/MIVB.raw	Virtual Machine image file	31.3 GB
6 file(s)		Total: 40.2 GB / Available: 3 GB

9. Open the **exdeploy.cfg** file using an editor (For example, Notepad) and change **CpuCount** to 3.
10. Save the **exdeploy.cfg** file.
11. Scroll down to the **Import File Through Web Browser** table, select **vm/images**, in the **Path** list, click **Choose File**, select the updated **exdeploy.cfg** file, and then click **Import**.

Import File Through Web Browser	
Path	File
vm/images/	Choose File exdeploy.cfg

Import

Note:

Do not copy the same **exdeploy.cfg** file to different EX systems as each EX has a unique date in the file.

12. After the **exdeploy.cfg** file is imported, click the **Reboot** tab and then click the **Reboot** button. The EX Controller Web GUI reboots.

Mitel | EX Controller

System Network SBC ISDN POTS SIP Media Telephony Call Router Management **Reboot**

• Reboot

Current Status

Please click on the Reboot button to reboot the device.

Warning: Your web session will be lost and you will be redirected to the login page after the reboot process.

Reboot

13. After the EX Controller Web GUI reboots, [Log in to the EX Controller Web GUI](#) on page 47.
14. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

15. In the **Virtual Machine Status** table, verify that the **Nb Cores** column for **exdeploy** shows **3**.

Mitel | EX Controller

System Network SBC ISDN POTS SIP Media Telephony Call Router Management Reboot

Information Services Hardware Endpoints Event Log Local Log Packet Capture Diagnostic VM

• Virtual Machines

Virtual Machine Status										
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State
exdeploy		12:37:91:0b:dc:b8	-1	All	e1000	1024	20	qcow2	1	Stopped
MIVB	mvf.iso	12:df:4c:0b:dc:b8	-1	All	virtio	2048	32	raw	3	Started

Virtual Machine Configuration								
Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions	
exdeploy		12:37:91:0b:dc:b8	-1	All	e1000	Manual	▶ ■ ▶ ⊞ ◀	
MIVB	mvf.iso	12:df:4c:0b:dc:b8	-1	All	virtio	Auto	▶ ■ ▶ ⊞ ◀	

Virtual Machine Creation					
Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	
			raw	1	+

16. If the **MiVB** virtual machine was already installed, then by default, the **exdeploy** virtual machine does not start after the EX Controller reboots. To start the **exdeploy** virtual machine, stop the **MiVB** virtual machine, wait and refresh the page until the **MiVB** virtual machine is stopped, and then start the **exdeploy** virtual machine.
17. If you want to deploy MiVoice Business or upgrade the EX Controller Deployment Tool, copy the downloaded files **exdeploy-x.x.x.x.zip** and **MiVB-9.x.x.x-yy.img.zip** from your deployment PC to the USB flash drive.
18. If you want to [assign a static IP address for the EX Controller Deployment Tool](#), then create a **lan.cfg** file with the static IP address and gateway IP address in the following format and copy the file to the USB flash drive:

addr=<static IP address/CIDR>

gateway=<IP address>

For example:

addr=10.38.75.41/24

gateway=10.38.75.1

19. Insert the USB flash drive into either port 6 or port 7 of the EX Controller. See [Connection Interfaces and LEDs](#) on page 14.
20. Continue with [Running the EX Controller Deployment Tool to Install the MiVoice Business Virtual Machine](#) on page 34.

Appendix D: Increasing the RAM size for MiVoice Business Virtual Machine

10

The deployment size of the MiVoice Business virtual machine on the EX Controller is increased to 3072 MB to accommodate the additional resources requirements for hosting the MPA blade. Increasing the RAM size is necessary only if you intend to install MPA.

The exdeploy tool versions 1.1.22.0 and later, by default, creates the MiVB VM with 3072 MB. You can follow this procedure to increase the RAM size for earlier versions of MiVoice Business for which the default RAM size for the MiVoice Business virtual machine is less than 3072 MB.

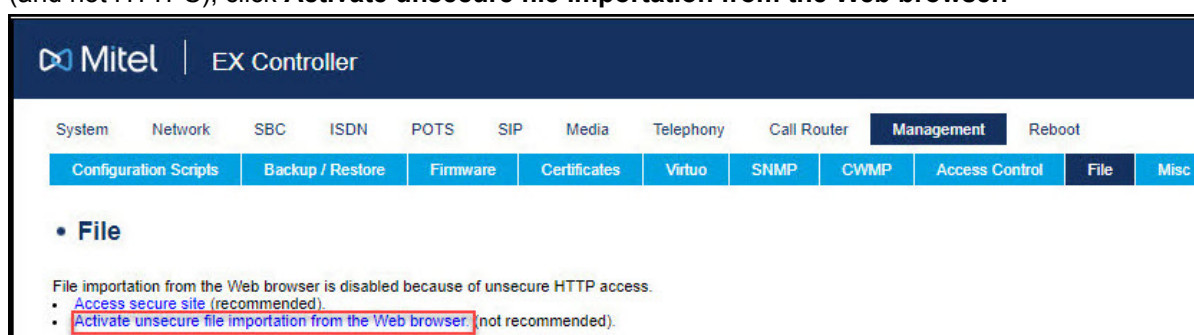
Note:

The extra memory is required for MPA blade to be run inside MiVoice Business Virtual Machine after the system is rebooted. When the existing system upgrades the EX Blade to MiVoice Business 9.4 and later, the MiVoice Business Virtual Machine configuration file on the EX Controller increases in size from 2048 MB to 3072 MB.

Procedure

Perform the following procedure to configure the size of the MiVoice Business VM to 3072 MB:

1. Log in to the EX Controller Web GUI.
2. Navigate to **Management > File**. If you are accessing the EX Controller using HTTP (and not HTTPS), click **Activate unsecure file importation from the Web browser**.



3. Scroll down to the VM files table, and click vm/images/MiVB.cfg to download the MiVB.cfg file to your PC.

VM files		
Name	Description	Size
vm/images/factory/exdeploy.cfg	Factory Virtual Machine configuration file (read-only)	1 KB
vm/images/factory/exdeploy.img	Factory Virtual Machine image file (read-only)	2.6 GB
vm/images/exdeploy.cfg	Virtual Machine configuration file	1 KB
vm/images/exdeploy.snapshot	Virtual Machine snapshot image file	6.3 GB
vm/images/MiVB.cfg	Virtual Machine configuration file	1 KB
vm/images/MiVB.raw	Virtual Machine image file	31.3 GB
6 file(s)		Total: 40.2 GB / Available: 3 GB

4. Open the MiVB.cfg file using an editor (For example, Notepad) and change MemorySizeMB to 3072.

5. Save the MIVB.cfg file.
6. Scroll down to the Import File Through Web Browser table, select vm/images, in the Path list, click Choose File, select the updated MIVB.cfg file, and then click Import.

Import File Through Web Browser	
Path	File
vm/images/	Choose File MIVB.cfg

[Import](#)

Note:

Do not copy the same MIVB.cfg file to different EX systems as each EX system has a unique date in the file.

7. After the MIVB.cfg file is imported, click the Reboot tab and then click the Reboot button. The EX Controller Web GUI begins to reboot.

The screenshot shows the Mitel EX Controller Web GUI. The top navigation bar includes tabs for System, Network, SBC, ISDN, POTS, SIP, Media, Telephony, Call Router, Management, and Reboot. The Reboot tab is selected and highlighted with a red box. Below the navigation bar, the 'Reboot' section is displayed. It contains a 'Current Status' box with the following text: 'Please click on the Reboot button to reboot the device.' and 'Warning: Your web session will be lost and you will be redirected to the login page after the reboot process.' A 'Reboot' button is located at the bottom right of the status box, also highlighted with a red box.

8. After the EX Controller Web GUI reboots, log in to the EX Controller Web GUI.
9. Navigate to System -> VM.

The Virtual Machine page is displayed.

10. In the Virtual Machine Status table, verify that the RAM (Mb) column for MiVB shows 3072.

Mitel | EX Controller

System

Network

SBC

ISDN

POTS

SIP

Media

Telephony

Call Router

Management

Reboot

Information

Services

Hardware

Endpoints

Event Log

Local Log

Packet Capture

Diagnostics

VM

Virtual Machines

Virtual Machine Status

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores	State
exdeploy		12:6d:9c:0b:dc:b8	-1	None	e1000	1024	20	qcow2	1	Stopped
MIVB	mvf.iso	12:ce:0d:0b:dc:b8	-1	All	virtio	3072	32	raw	3	Started

Virtual Machine Configuration

Vm Name	Iso Name	MAC Address	Vnc Id	Usb	Network Adapter	Startup	Actions
exdeploy		12:6d:9c:0b:dc:b8	-1	None	e1000	Manual	
MIVB	mvf.iso	12:ce:0d:0b:dc:b8	-1	All	virtio	Auto	

Virtual Machine Creation

Vm Name	Ram (Mb)	Storage (Gb)	Image Format	Nb Cores
			raw	1

Appendix E- Programming Enterprise Gateway Trunks and Analogue FXS Ports

11

Programming Enterprise Gateway Trunks

The Enterprise Gateways form is used to configure the IP address and the SNMP details of the EX controller.

Note:

This form is applicable only to the EX Controller.

Before You Begin

Ensure you have the following information:

- When you add an EX Controller to the Enterprise Gateways form, if the Auto Program Trunk Profiles option is selected:
 1. The system identifies the available endpoints on the EX controller and a trunk profile for each type of trunk endpoint is created.
 2. The trunk endpoints in the Gateway Trunks form are auto-assigned to each of the trunk profiles based on the trunk types.
 3. SIP Peer Network Elements and SIP Peer Profiles are created with the same names as the Gateway Trunk Profiles.

Conditions

- The data changes performed on the Mediatrix Web Management Interface are not reflected in the System Administration tool or the Server Manager.
- You can only program one EX controller using this form.
- You cannot delete the entry for the local Enterprise Gateway.
- Use the SNMP credentials to configure the EX Controller.

Programming PRI

Fill out the forms below in the order listed.

1. Trunk Attributes form - to check for an unused Trunk Attribute entry click **Trunks > Trunk Attributes**.

2. Gateway Trunk Descriptors form -

- To program click Trunks > Enterprise Gateways > Gateway Trunk Descriptors from the left navigation pane.
- Click the unprogrammed entry and click Change
- Configure the line type to T1 or E1

Note:

If you change Line Type, the EX Controller (host) needs to be rebooted.

- Configure Signaling to Isdn, R2, or Eam
- Configure Endpoint Type to Te or Nt
- Click Save

3. Gateway Trunk Profiles form -

- To program click Trunks > Enterprise Gateways > Gateway Trunk Profiles from the left navigation pane.
- Click Add, enter the Name, enter the unused Trunk Service Number.
- Click Save.

4. Gateway Trunks form -

- To program click Trunks > Enterprise Gateways > select an entry > change the E1T1 endpoint and select the Gateway Trunk Profiles name

5. Gateway Configuration Scripts form -

- To program click Trunks > Enterprise Gateways > Gateway Configuration Scripts.
- Select slot
- Click on the drop down menu of the Default Configuration Files, to select an appropriate
- Mitel per slot for the PSTN circuit
- Click Execute

6. ARS Routes - ARS continues to be provisioned in the traditional manner by assigning a route to a digit or digit string. Complete the following fields in this form:

- Select SIP Trunk/Enterprise Gateway from the pull-down list in Routing Medium.
- Select a Gateway Trunk Profile name from the SIP Peer Profile pull-down list.

Programming FXO

Fill out the forms below in the order listed.

1. Trunk Attributes form - To check for an unused Trunk Attribute entry click Trunks > Trunk Attributes.

2. Gateway Trunk Descriptors form - To view the status click Trunks > Gateway Trunk Descriptors > select an entry > click Change.

3. Gateway Trunk Profiles form -

- To program click Trunks > Enterprise Gateways > Gateway Trunk Profiles from the left navigation pane
- Click Add, enter the Name, enter the unused Trunk Service Number
- Click Save

4. Gateway Trunks form - To program click Trunks > Enterprise Gateways > select/change the FXO endpoint and select the Gateway Trunk Profiles name.
5. Gateway Configuration Scripts form (Optional)
 - To program click Trunks > Enterprise Gateways > Gateway Configuration Scripts.
 - Select slot
 - Click on the drop down menu of the Default configuration files, to select an appropriate Mitel per slot for the PSTN circuit
 - Click Execute
6. ARS Routes - ARS continues to be provisioned in the traditional manner by assigning a route to a digit or digit string. Complete the following fields in this form:
 - Select SIP Trunk/Enterprise Gateway from the pull-down list in Routing Medium.
 - Select a Gateway Trunk Profile name from the SIP Peer Profile pull-down list.

Note:

After successfully adding a Gateway Trunk Profile, Network Elements and SIP Peer Profile forms will have entries with the same Gateway Trunk Profiles name.

Programming Analogue FXS Ports

The User and Services Configuration form combines the functions of several system forms into a single form; however, you can still access and use the individual forms.

Programming

Fill out the form User and Service Configuration to program Analogue FXS Port:

- Click User and Devices > User and Services Configuration from the left navigation pane.
- To add a phone, click Add > select Default User and Device
- Click on the tab User Profile > enter the name
- Click on the tab Service Profile > enter the number. Set the device type to AnalogFXS
- Click on the tab Device Details. By default the first Endpoint ID is selected but, you can manually select the required Endpoint ID from the drop down.
- Click Save Changes.

FXS Line Length Specifications

This section provides details regarding the FXS line length and related considerations.

Standard FXS Port Line Length:

- 450 meters, calculated for a 26 AWG wire.

Long Loop FXS-LP Port Line Length:

- 2000 meters, calculated for a 26 AWG wire.

Note: For longer loop applications, the Ringer Equivalency Number (REN) must be reduced to a maximum of 3 REN to maintain an acceptable ringing voltage at the equipment.

Other FXS-LP Considerations:

- The FXS-LP card includes secondary protection to guard against surges and lightning.
- For external cable applications, the customer must install primary protection (typically at the building entrance).
- The FXS-LP card can support a loop with up to 1200 ohms of DC impedance (including cable impedance, connected equipment impedance, protections, etc.).
- The FXS-LP card features a short-loop SLIC with a longitudinal Balance of approximately 45dB, while long-loop SLICs typically offer 58dB. As a result, common-mode noise may induce additional noise on longer loops.
- Longer loops may degrade FXS-LP AC performance. To compensate for this, different sets of AC coefficients may be required.
- When using a 24 AWG wire, an estimated 20% to 25% distance increase can be expected.

Analog Phones on VOIP Gateway FXS port

The maximum number of analog phones that can be connected on a VOIP Gateway FXS port:

- Standard FXS Port:
 - 5 REN for short distances (<300 meters), 45Vrms
 - 4 REN for standard distances (<450 meters), 45Vrms
- Long Loop FXS-LP Port:
 - 3 REN for long distances (<3000 meters), 60Vrms

Appendix F - Enabling/Disabling VNC Capability and Resetting the MSL Password

12

This chapter contains the following sections:

- [Enabling the VNC Capability](#)
- [Disabling the VNC Capability](#)
- [Resetting the MSL password](#)

12.1 Enabling the VNC Capability

To enable VNC for the exdeploy virtual machine or MIVoice Business virtual machine:

1. [Log in to the EX Controller Web GUI](#) on page 47.
2. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

3. Click  to stop the required virtual machine
4. Do the following:
 - a. For the **VM Name** field **exdeploy**, in the **VNC Id** field, enter **0**.
 - b. For the **VM Name** field **MIVB**, in the **VNC Id** field, enter **1**.

 **Note:** Any value of 0 or greater enables VNC access for that VM.

5. Click **Apply** to apply the changes.
6. Click  to start the virtual machine.

 **Note:** If you enable VNC, it might open a security hole and recommend disabling it for a secure system.

12.2 Disabling the VNC Capability

To disable VNC for the exdeploy virtual machine or MIVoice Business virtual machine:

1. [Log in to the EX Controller Web GUI](#) on page 47.

2. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

3. Click  to stop the required virtual machine
4. Do the following:

- a. For the **VM Name** field **exdeploy**, in the **VNC Id** field, enter **-1**.
- b. For the **VM Name** field **MIVB**, in the **VNC Id** field, enter **-1**.

 **Note:** Setting the VNC ID to -1 will disable VNC access for that VM.

5. Click **Apply** to apply the changes.
6. Click  to start the virtual machine.

12.3 Resetting the MSL password

To reset MSL root/admin password:

1. [Log in to the EX Controller Web GUI](#) on page 47.
2. Navigate to **System > VM**.

The **Virtual Machine** page is displayed.

3. Click  to stop the required virtual machine
4. For the **VM Name** field **MIVB**, in the **VNC Id** field, enter **1**.

 **Note:** Setting the VNC ID to 1 will enable VNC access for that VM.

5. Click **Apply** to apply the changes.
6. Click  to start the virtual machine.
7. When the Grub menu screen appears, on the first entry of the grub menu, Press the **e** key to access the Grub editor.

 **Note:** You must access VNC promptly after starting the virtual machine, because the menu likely remains available for only 10 seconds.

8. In the shell of the grub editor, scroll down to the line that begins with "Linux".
9. Using the arrow key to navigate to the end of the "Linux" line (.../lv_swap) and enter the command:
rd.break enforcing=0.
10. Press **CLTR + X** to access the emergency mode.

11. To reset password in emergency mode:

- a. Enter the following command: `mount -o rw,remount /sysroot.`
- b. Enter the following command: `chroot /sysroot.`
- c. Enter the following command: `passwd root.`
- d. Follow the prompt to enter the new root password.
- e. Enter the following command: `passwd admin.`
- f. Follow the prompt to enter the new admin password.
- g. Enter the following command: `touch /.autorelabel`
- h. Enter the following command to exit the /sysroot environment: `exit`
- i. Enter the following command to leave the switch root: `exit #`
- j. Enter the following command to reboot the system: `reboot -f`

i Note: Perform these if you are using a MiVoice Business system 10.1 and later versions. To reset the MSL password using a MiVoice Business system 10.0 and previous versions using Rocky 8 or Centos 7:

1. Perform [steps 1 - 6](#).
2. When the GRUB boot loader splash screen appears momentarily, press the **a** key.

The load process stops, enabling you to append arguments to the kernel boot line.

3. In the kernel boot line, type " **s**" (note the leading space) and press **Enter**.
4. From the command prompt, enter the following command: `mount / -o remount,rw`

This will remount the file system as read/write, as by default single user mode is read only.

5. Enter the following command: `passwd root.`
6. Follow the prompt to enter the new root password.
7. Enter the following command: `passwd admin.`
8. Follow the prompt to enter the new admin password.
9. Enter the following command to reboot the system: `reboot -f`

You should now be able to log in normal to the command prompt as admin or root, and can log in to the server manager as admin, with the new passwords.

Appendix G - EX-Controller Link Redundancy support

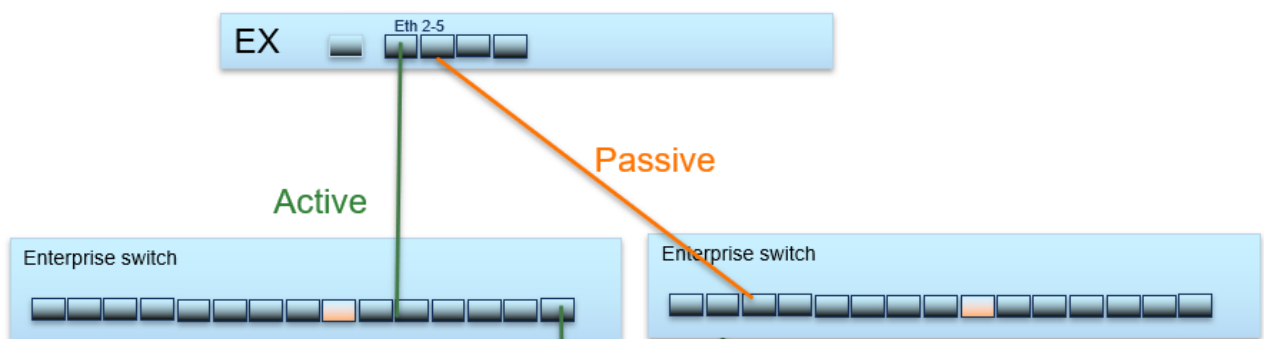
13

Overview

The IP Link Redundancy feature provides high availability for Ethernet connectivity by allowing a dual-link setup using **ETH4** and **ETH5** on the EX Controller. This setup designates one port as the **primary (active)** link and the other as a **secondary (passive)** backup. If the active link fails, traffic automatically switches to the passive link, ensuring continuous network connectivity.

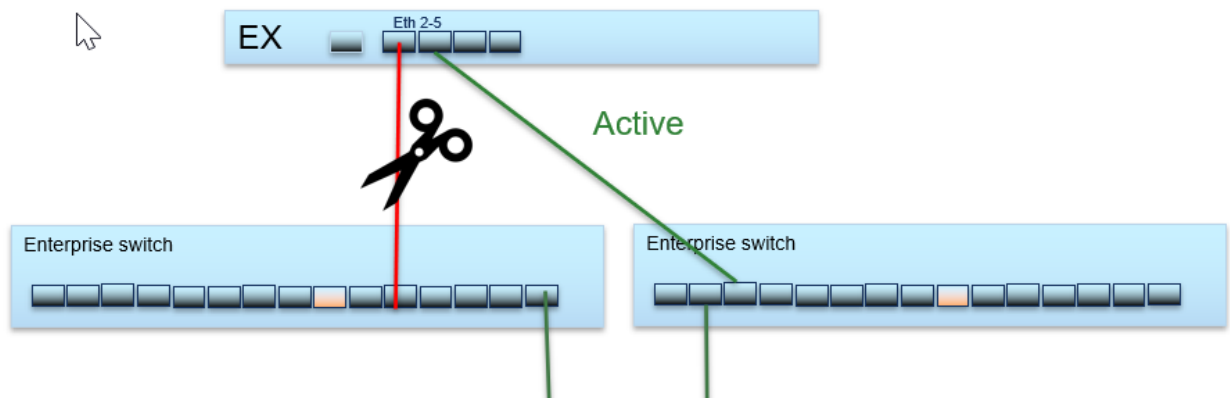
Normal operation:

In the normal state, ETH4 is the designated **primary (active)** interface. All network traffic is routed through ETH4, while ETH5 remains passive and disabled. This ensures a stable connection and prevents any risk of a network loop. The system continuously monitors ETH4 for link status.



Failover scenario:

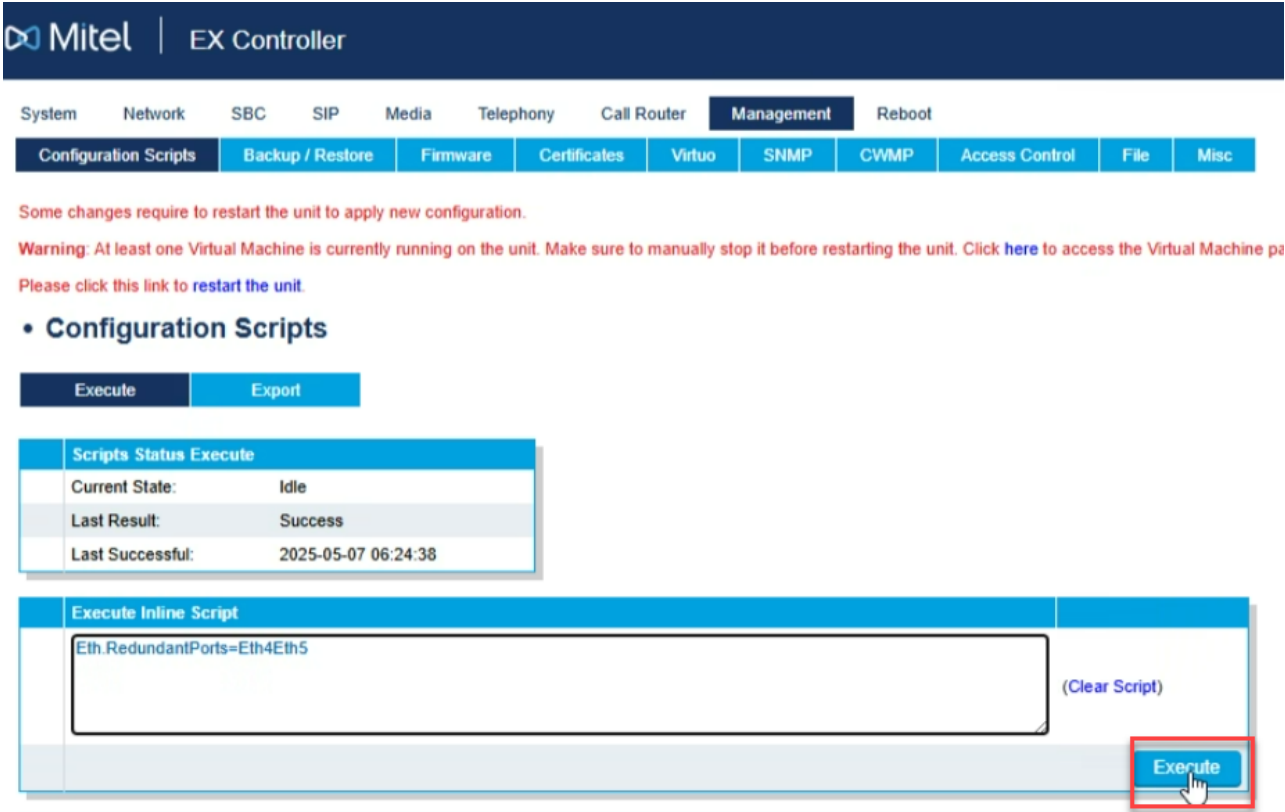
When the **ETH4** link is physically disconnected or fails, the system detects the loss and **automatically activates ETH5** as the backup link. The **ETH5** becomes active automatically within **1 to 3 seconds** (500 ms polling interval). Network traffic is seamlessly rerouted through ETH5 to maintain connectivity. ETH5 remains active until ETH4 is restored, at which point the system reverts to ETH4.



Configuration via Web Interface

To configure the IP Link Redundant Ethernet Ports Feature, do the following:

- 1. Navigate to: **Management > Configuration Scripts > Execute.**
- 2. In **Execute Inline Script** field, enter **Eth.RedundantPorts=Eth4Eth5.**
- 3. Click **Execute.**



- 4. **Reboot** the unit to apply the configuration.

Note: The **Eth.RedundantPorts=Eth4Eth5** command can be used to configure via Command Line Interface (CLI) or SNMP.

Redundant ports parameter details

To configure the redundant ports, the following parameters are used:

Parameter	Value
Type	Enum

Parameter	Value
Range	Disable(0) Eth4Eth5(100) <i>Note:</i> Disable: Redundant Ports is disabled. Eth4Eth5: Redundant Ports is enabled.
Default	Disable
SNMP OID	.1.3.6.1.4.1.4935.1000.100.200.100.2400.1.10100.100

